

Encyclopedia of Criminal Activities and the Deep Web

Mehdi Khosrow-Pour, D.B.A.
Information Resources Management Association, USA

Volume I

Section 1: Cybercriminal Profiles, Understanding Cybercrime, and the Realities of the Dark Web

Section 2: Cyber Warfare, Cybersecurity, Spyware, and Regulatory Policies and Solutions

Section 3: Drug Trafficking, Human Trafficking, and the Sexual Exploitation of Children

A volume in the Advances in Criminology,
Criminal Justice, and Penology (ACCJP) Book
Series

IGI Global
DISSEMINATOR OF KNOWLEDGE

Published in the United States of America by

IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2020 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Names: Khosrow-Pour, Mehdi, 1951- editor.

Title: Encyclopedia of criminal activities and the Deep Web / Mehdi

Khosrow-Pour, D.B.A., editor.

Description: Hershey, PA : Information Science Reference, [2020]

Identifiers: LCCN 2019006534 | ISBN 9781522597155 (hardcover) | ISBN

9781522597162 (ebook)

Subjects: LCSH: Computer crimes. | Dark Web.

Classification: LCC HV6773 .E529 2020 | DDC 364.16/8--dc23 LC record available at <https://lcn.loc.gov/2019006534>

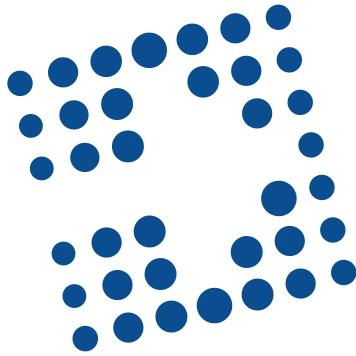
This book is published in the IGI Global book series Advances in Criminology, Victimology, Serial Violence, and the Deep Web (ACVSVDW) (ISSN: pending; eISSN: pending)

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.



Advances in Criminology, Criminal Justice, and Penology (ACCJP) Book Series

Liam J. Leonard
Northern Arizona University, USA

ISSN:pending
EISSN:pending

MISSION

Criminology has never been more relevant. Violence, serial murder, crime and victimization continue to remain an unfortunate staple of society. Crime is a key issue globally, nationally, and regionally. Law enforcement personnel within the criminal justice system must keep pace with ever changing modes of crime. As officials work to predict and prevent crimes, as well as apprehend offenders, they will need to devise new tools and strategies to preserve the safety of society and ensure proper justice is served.

The **Advances in Criminology, Criminal Justice, and Penology (ACCJP)** Book Series explores emerging research behind crime control strategies, crime motivation, new methods and the utilization of technology for committing illegal acts, criminal justice and reform strategies, and the effects of crime on society and its victims. The publications contained within this series are valuable resources for government officials, law enforcement officers, corrections officers, prison management, criminologists, sociologists, psychologists, forensic scientists, security specialists, academicians, researchers, and students seeking current research on international crime.

COVERAGE

- Policing
- Restorative Justice
- Fraud
- Criminal Psychology
- Penal System
- Criminal Justice Systems
- Serial Murder
- Human Trafficking
- Criminology
- Law

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: <http://www.igi-global.com/publish/>.

The Advances in Criminology, Criminal Justice, and Penology (ACCJP) Book Series (ISSN pending) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit <http://www.igi-global.com/book-series/advances-criminology-criminal-justice-penology/212650>. Postmaster: Send all address changes to above address. Copyright © 2020 IGI Global. All rights, including translation in other languages reserved by the publisher. No part of this series may be reproduced or used in any form or by any means – graphics, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems – without written permission from the publisher, except for non commercial, educational use, including classroom teaching purposes. The views expressed in this series are those of the authors, but not necessarily of IGI Global.

Titles in this Series

For a list of additional titles in this series, please visit: www.igi-global.com/book-series

Comparative Criminology Across Western and African Perspectives

Simeon Peter Sungi (United States International University-Africa, Kenya) Nabil Ouassini (Dixie State University, USA) and Joyce Muchemi (Mount Kenya University, Kenya)

Information Science Reference • ©2020 • 300pp • H/C (ISBN: 9781799828563) • US \$225.00

Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support

Augusto Balloni (Italian Society of Victimology, Italy) and Raffaella Sette (University of Bologna, Italy)

Information Science Reference • ©2020 • 553pp • H/C (ISBN: 9781799812869) • US \$245.00

Global Perspectives on Victimization Analysis and Prevention

Johnson Oluwole Ayodele (Lagos State University, Nigeria)

Information Science Reference • ©2020 • 272pp • H/C (ISBN: 9781799811121) • US \$195.00

Handbook of Research on Mass Shootings and Multiple Victim Violence

Gordon A. Crews (University of Texas Rio Grande Valley, USA)

Information Science Reference • ©2020 • 531pp • H/C (ISBN: 9781799801139) • US \$265.00

Sexual Violence and Effective Redress for Victims in Post-Conflict Situations Emerging Research and Opportunities

Jean de Dieu Sikulibo (University of Lay Adventists of Kigali, Rwanda)

Information Science Reference • ©2019 • 328pp • H/C (ISBN: 9781522581949) • US \$145.00

Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention

Sunita Vikrant Dhavale (Defence Institute of Advanced Technology, India)

Information Science Reference • ©2019 • 281pp • H/C (ISBN: 9781522576280) • US \$220.00



701 East Chocolate Avenue, Hershey, PA 17033, USA

Tel: 717-533-8845 x100 • Fax: 717-533-8661

E-Mail: cust@igi-global.com • www.igi-global.com

This book is dedicated to the memory of my late father for the love and care that he always displayed for his family, and for teaching me the importance of humanitarianism. Also, to my wife, Olga, and our son, Darius, for filling my life with so much love, joy, and happiness.

List of Contributors

Ajayi, Mofoluwake / <i>Covenant University, Nigeria</i>	210
Al Shibli, Murad / <i>Abu Dhabi Polytechnic, UAE</i>	1089
Algawi, Asaf / <i>University of Jyväskylä, Finland</i>	1136
Almeida, Fernando / <i>Polytechnic Institute of Gaya, Portugal</i>	749
Amarasekara, Bede Ravindra / <i>Massey University, New Zealand</i>	1062
Amodu, Lanre / <i>Covenant University, Nigeria</i>	823
Anastasiou, Athanasios / <i>National Technical University of Athens, Greece</i>	763
Androutsou, Thelma / <i>National Technical University of Athens, Greece</i>	763
Anglim, Christopher Thomas / <i>University of the District of Columbia, USA</i>	402
Ara, Fardaus / <i>Rajshahi University, Bangladesh</i>	699
Awofeso, Niya / <i>School of Health and Environmental Studies, Hamdan Bin Mohammed Smart University, UAE</i>	318
Ayedun, Caleb Abiodun / <i>Covenant University, Nigeria</i>	210
Azhar, Sandal / <i>University of Delhi, India</i>	905
Badia, Antonio / <i>University of Louisville, USA</i>	1053
Baeva, Liudmila Vladimirovna / <i>Astrakhan State University, Russia</i>	660
Baldwin, Leroy / <i>Atlanta Metropolitan State College, USA</i>	606
Bali, Aakash / <i>JayPee University of Information Technology, Solan, India</i>	788
Balusamy, Balamurugan / <i>Galgotias University, India</i>	1
Bansal, Himani / <i>Jaypee University, Solan, India</i>	864
Barbato, Simone / <i>Idego Psicologia Digitale, Italy</i>	668
Barnor, Jonathan Nii Barnor / <i>University of Ghana Business School, Ghana</i>	66
Bedi, Punam / <i>University of Delhi, India</i>	152
Bell, Monica M. / <i>University of Notre Dame, USA</i>	547
Ben Yehuda, Raz / <i>University of Jyväskylä, Finland</i>	1150
Benson, Vladlena / <i>Aston Business School, UK</i>	979
Boateng, Richard / <i>University of Ghana Business School, Ghana</i>	66, 945
Brandtweiner, Roman H. / <i>Vienna University of Economics and Business, Austria</i>	628
Broni, Frederick Edem / <i>University of Ghana Business School, Ghana</i>	945
Byrd, Joshua E. / <i>American Intercontinental University, USA</i>	606
Can, Muhammed / <i>University of Minho, Portugal</i>	271
Chea, Chiam Chooi / <i>Open University Malaysia, Malaysia</i>	932
Chen, Xingyu / <i>Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i> ..	52, 965
Chhapola, Vikas / <i>University of Delhi, India</i>	905

Costarides, Vassilia / <i>Institute of Communication and Computer Systems (ICCS), Greece</i>	763
Crowell, Charles R. / <i>University of Notre Dame, USA</i>	547
DaCosta, Boaventura / <i>Solers Research Group, USA</i>	881
DeDominicis, Benedict E. / <i>Catholic University of Korea, South Korea</i>	242
Di Natale, Lorenzo / <i>Idego Psicologia Digitale, Italy</i>	668
Dornfeld, László / <i>Ferenc Mádl Institute of Comparative Law, Hungary</i>	565
Elangovan, Ramanujam / <i>Thiagarajar College of Engineering, India</i>	129
Elkins, Aaron / <i>San Diego State University, USA</i>	497
Er, Verity / <i>Home Team Behavioural Sciences, Ministry of Home Affairs, Singapore</i>	52
Exposito, Julie A. / <i>Nova Southeastern University, USA</i>	177
Fasanya, Opeyemi / <i>Covenant University, Nigeria</i>	823
Frost, Eric / <i>San Diego State University, USA</i>	497
Gamidullaeva, Leyla / <i>Penza State University, Russia</i>	1034, 1043
Gangwar, Suraj / <i>University of Delhi, India</i>	23
Gargaglione, Giulia / <i>Idego Psicologia Digitale, Italy</i>	668
Giannouli, Dimitra / <i>Computer Solutions SA, Greece & University of Leeds, UK</i>	763
Girma, Anteneh T. / <i>University of District of Columbia, USA</i>	837
Goh, Pamela / <i>Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	52, 965
Gudoshava, Dylas / <i>Zimbabwe Open University, Zimbabwe</i>	732
Gupta, Daya Sagar / <i>Shershah College of Engineering Sasaram Bihar, India</i>	1112
Gupta, Neha / <i>University of Delhi, India</i>	152
Hansen, Laura Pinto / <i>Western New England University, USA</i>	258
Herschel, Richard T. / <i>Saint Joseph's University, USA</i>	140
Hoanca, Bogdan / <i>University of Alaska, Anchorage, USA</i>	36
Hohemberger, Rumenigüe / <i>Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	893
Holland, Barbara Jane / <i>Brooklyn Public Library, USA</i>	108
Huber, Edith / <i>Danube University Krems, Austria</i>	193, 628
Hultgren, Marisa / <i>San Diego State University, USA</i>	497
Jaha, Farida / <i>LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco</i>	1123
Janicke, Helge / <i>De Montfort University, UK</i>	287
Jegede, Ajibade Ebenezer / <i>Covenant University, Nigeria</i>	210
Jennex, Murray Eugene / <i>San Diego State University, USA</i>	497
Jindal, Vinita / <i>Keshav Mahavidyalaya, University of Delhi, India</i>	152
Jones, Kevin / <i>Airbus, UK</i>	287
Kajzer, Mitchell D. / <i>University of Notre Dame, USA</i>	547
Kanarev, Sergey / <i>Penza State University, Russia</i>	1034
Kartit, Ali / <i>LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco</i>	1123
Kaur, Prabhjyot / <i>University of Delhi, India</i>	463
Kaushal, Puneet / <i>Lucideus Technologies, India</i>	919
Kaushal, Puneet Kumar / <i>Lucideus Technologies, India</i>	463
Kayode-Adedeji, Tolulope / <i>Covenant University, Nigeria</i>	823
Kejriwal, Mayank / <i>University of Southern California, USA</i>	478
Khader, Majeed / <i>Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i> 52	
Khan, Nasreen / <i>Multimedia University, Malaysia</i>	435, 518

Khan, Shereen / <i>Multimedia University, Malaysia</i>	435, 518
Khan, Tehmina / <i>RMIT University, Australia</i>	591
Kiperberg, Michael / <i>Holon Institute of Technology, Israel</i>	1136
Konzen, Marcos Paulo / <i>Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	893
Köroğlu, Muhammet Ali / <i>Uşak University, Turkey</i>	229
Lambrecht, Ana / <i>Universidad Nacional de Río Negro, Argentina</i>	362
Lamidi, Mufutau Temitayo / <i>University of Ibadan, Nigeria</i>	1018
Leon, Roe / <i>University of Jyväskylä, Finland</i>	1150
Leon, Roe Shimon / <i>University of Jyväskylä, Finland</i>	1136
Lourenço, Justino / <i>Polytechnic Institute of Gaya, Portugal</i>	749
Luchessi, Lila / <i>Universidad Nacional de Río Negro, Argentina & Universidad de Buenos Aires, Argentina</i>	362
Maglaras, Leandros / <i>De Montfort University, UK</i>	287
Marmo, Roberto / <i>University of Pavia, Italy</i>	810
Mathrani, Anuradha / <i>Massey University, New Zealand</i>	1062
Matteson, Cortney E. / <i>Orange County School District, USA</i>	177
Matteson, Rande W. / <i>Nova Southeastern University, USA</i>	177
McMurtry, Anita W. / <i>Atlanta Metropolitan State College, USA</i>	334
Miccoli, Maria Rosa / <i>Idego Psicologia Digitale, Italy</i>	668
Mkrttchian, Vardan / <i>HHH University, Australia</i>	1034, 1043
Mock, Kenrick J. / <i>University of Alaska, Anchorage, USA</i>	36
Mohammed, Anne-Marie / <i>The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	979
Mpasdeki, Maria / <i>NGO Solidarity Now, Athens, Greece</i>	580
Mukherjee, Sovik / <i>St. Xavier's University, Kolkata, India</i>	93
Narang, Vinayak / <i>University of Delhi, India</i>	23
Neo, Loo Seng / <i>Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i> ..	52, 965, 1003
O'Donnell, Eileen / <i>Technological University Dublin, Ireland</i>	615
O'Donnell, Liam / <i>Technological University Dublin, Ireland</i>	615
Okeke, Obianuju Victoria / <i>Covenant University, Nigeria</i>	823
Okorie, Nelson / <i>Covenant University, Nigeria</i>	210, 823
Owusu, Acheampong / <i>University of Ghana Business School, Ghana</i>	945
Oyero, Olusola / <i>Covenant University, Nigeria</i>	210
Palanimuthu, Suresh / <i>Galgotias University, India</i>	1
Phan, Raphael C. W. / <i>Multimedia University, Malaysia</i>	435, 518
Pitoglou, Stavros / <i>National Technical University of Athens, Greece & Computer Solutions SA, Greece</i>	763
Pospisil, Bettina / <i>Danube University Krems, Austria</i>	193
Premat, Christophe Emmanuel / <i>Stockholm University, Sweden</i>	347
Quirchmayr, Gerald / <i>University of Vienna, Austria</i>	193
R., Parthasarathi / <i>Delhi University, India</i>	919
Ramdeo, Shalini / <i>The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	304, 686
Rathee, Anu / <i>Maharaja Agrasen Institute of Technology, India</i>	1
Rauhala, Juhani / <i>University of Jyväskylä, Finland</i>	990

Rehman, Tansif Ur / <i>University of Karachi, Pakistan</i>	412, 424
Resh, Amit / <i>Shenkar College, Israel</i>	1136
Robinson, Michael / <i>Airbus, UK</i>	287
Rodriguez, Nathan John / <i>Weber State University, USA</i>	715
Ross, David B. / <i>Nova Southeastern University, USA</i>	177
Rossi, Fabio Diniz / <i>Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	893
Rotelli, Valentina / <i>Idego Psicologia Digitale, Italy</i>	668
Saridakis, George / <i>University of Kent, UK</i>	979
Sasso, Melissa T. / <i>Nova Southeastern University, USA</i>	177
Scogings, Chris / <i>Massey University, New Zealand</i>	1062
Seboeck, Walter / <i>Danube University Krems, Austria</i>	193
Segerson, Jamie / <i>University of Notre Dame, USA</i>	547
Seok, Soonhwa / <i>Korea University, South Korea</i>	881
Shahi, Manisha / <i>University of Delhi, India</i>	905
Silvestri, Valentina / <i>University of Milan-Bicocca, Italy</i>	668
Singh Tomar, Deepak / <i>Maulana Azad National Institute of Technology, Bhopal, India</i>	788, 864
Singh, Riann / <i>The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	304, 686
Steinebach, Martin / <i>Fraunhofer SIT, Germany</i>	165
Stewart, Larry D. / <i>Atlanta Metropolitan State College, USA</i>	334
Tan, Olivia Swee Leng / <i>Multimedia University, Malaysia</i>	435, 518
Temp, Daniel Chaves / <i>Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	893
Thangamuthu, Poongodi / <i>Galgotias University, India</i>	1
Thomas, Ciza / <i>Directorate of Technical Education, India</i>	1077
Tiwari, Sachin / <i>Jawaharlal Nehru University, India</i>	374
Todd, Curtis L. / <i>Atlanta Metropolitan State College, USA</i>	334, 606
Tsiftzis, Zafeiris / <i>University of Bolton, UK</i>	580
Tyrväinen, Pasi / <i>University of Jyväskylä, Finland</i>	990
Ur Rahman, Rizwan / <i>Maulana Azad National Institute of Technology, Bhopal, India</i>	788, 864
Vergara, Rossanne Gale / <i>Multimedia University, Malaysia</i>	435, 518
Verma, Rishu / <i>Jaypee University of Information Technology, India</i>	864
Villano, Michael / <i>University of Notre Dame, USA</i>	547
Wadhwa, Danish / <i>JayPee University of Information Technology, Solan, India</i>	788
Wallace, Lacey Nicole / <i>Penn State Altoona, USA</i>	533
Wang, Ping / <i>Robert Morris University, USA</i>	837
Wegner, Veronica / <i>University of Notre Dame, USA</i>	547
Wesley, David T. A. / <i>Northeastern University, USA</i>	392
Whitney, Jessica / <i>San Diego State University, USA</i>	497
Wright, Michelle F. / <i>Penn State University, USA</i>	640
Yu, John / <i>Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	52
Yu, Szde / <i>Wichita State University, USA</i>	851
Zaidenberg, Nezer / <i>College of Management Academic Studies, Israel</i>	990
Zaidenberg, Nezer Jacob / <i>College of Management, Israel</i>	449, 1136, 1150
Zenk, Julaine / <i>University of Notre Dame, USA</i>	547

Table of Contents by Volume

Preface	xxviii
----------------------	--------

Acknowledgment	xxxv
-----------------------------	------

Volume I

Section 1: Cybercriminal Profiles, Understanding Cybercrime, and the Realities of the Dark Web

Cybercrime.....	1
-----------------	---

Poongodi Thangamuthu, Galgotias University, India
Anu Rathee, Maharaja Agrasen Institute of Technology, India
Suresh Palanimuthu, Galgotias University, India
Balamurugan Balusamy, Galgotias University, India

A Survey on Emerging Cyber Crimes and Their Impact Worldwide	23
--	----

Suraj Gangwar, University of Delhi, India
Vinayak Narang, University of Delhi, India

Artificial Intelligence-Based Cybercrime	36
--	----

Bogdan Hoanca, University of Alaska, Anchorage, USA
Kenrick J. Mock, University of Alaska, Anchorage, USA

Crime-Fake News Nexus	52
-----------------------------	----

Xingyu Chen, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore
John Yu, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore
Pamela Goh, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore
Loo Seng Neo, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore
Verity Er, Home Team Behavioural Sciences, Ministry of Home Affairs, Singapore
Majeed Khader, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Unveiling Cybercrime in a Developing Country	66
<i>Richard Boateng, University of Ghana Business School, Ghana</i>	
<i>Jonathan Nii Barnor Barnor, University of Ghana Business School, Ghana</i>	
Left-Wing Extremism From the Indian Perspective: An Econometric Interpretation	93
<i>Sovik Mukherjee, St. Xavier's University, Kolkata, India</i>	
Transnational Cybercrime: The Dark Web	108
<i>Barbara Jane Holland, Brooklyn Public Library, USA</i>	
The Dark Web: Hidden Access to Internet Today	129
<i>Ramanujam Elangovan, Thiagarajar College of Engineering, India</i>	
Privacy, Ethics, and the Dark Web.....	140
<i>Richard T. Herschel, Saint Joseph's University, USA</i>	
Dark Web: A Boon or a Bane	152
<i>Punam Bedi, University of Delhi, India</i>	
<i>Neha Gupta, University of Delhi, India</i>	
<i>Vinita Jindal, Keshav Mahavidyalaya, University of Delhi, India</i>	
File-Sharing and the Darknet.....	165
<i>Martin Steinebach, Fraunhofer SIT, Germany</i>	
Academic Integrity of Global Digital Masked Bandits Lurking the Deep and Dark Web	177
<i>David B. Ross, Nova Southeastern University, USA</i>	
<i>Julie A. Exposito, Nova Southeastern University, USA</i>	
<i>Melissa T. Sasso, Nova Southeastern University, USA</i>	
<i>Cortney E. Matteson, Orange County School District, USA</i>	
<i>Rande W. Matteson, Nova Southeastern University, USA</i>	
Modus Operandi in Cybercrime	193
<i>Bettina Pospisil, Danube University Krems, Austria</i>	
<i>Edith Huber, Danube University Krems, Austria</i>	
<i>Gerald Quirchmayr, University of Vienna, Austria</i>	
<i>Walter Seboeck, Danube University Krems, Austria</i>	
Necessity of Paradigm Shift in Criminological Theorizing.....	210
<i>Ajibade Ebenezer Jegede, Covenant University, Nigeria</i>	
<i>Olusola Oyero, Covenant University, Nigeria</i>	
<i>Nelson Okorie, Covenant University, Nigeria</i>	
<i>Caleb Abiodun Ayedun, Covenant University, Nigeria</i>	
<i>Mofoluwake Ajayi, Covenant University, Nigeria</i>	
Development of Crime Sociology From Bureaucratic Iron Cage to Digital Determination	229
<i>Muhammet Ali Köroğlu, Uşak University, Turkey</i>	

Section 2: Cyberwarfare, Cybersecurity, Spyware, and Regulatory Policies and Solutions

The Globalization of Hybrid Warfare and the Need for Plausible Deniability.....	242
<i>Benedict E. DeDominicis, Catholic University of Korea, South Korea</i>	
The Spy Who Never Has to Go Out Into the Cold Cyber Espionage	258
<i>Laura Pinto Hansen, Western New England University, USA</i>	
Grey Zone Conflicts in Cyber Domain: Nonlocality of Political Reality in the World of “Hyperobjects”	271
<i>Muhammed Can, University of Minho, Portugal</i>	
Developing Cyber Buffer Zones	287
<i>Michael Robinson, Airbus, UK</i>	
<i>Kevin Jones, Airbus, UK</i>	
<i>Helge Janicke, De Montfort University, UK</i>	
<i>Leandros Maglaras, De Montfort University, UK</i>	
The Management of Whistleblowing.....	304
<i>Riann Singh, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
<i>Shalini Ramdeo, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
Whistleblowing to Expose Criminal Activity in the Health Sector	318
<i>Niyi Awofeso, School of Health and Environmental Studies, Hamdan Bin Mohammed Smart University, UAE</i>	
Online Activism to Cybercrime	334
<i>Anita W. McMurtry, Atlanta Metropolitan State College, USA</i>	
<i>Larry D. Stewart, Atlanta Metropolitan State College, USA</i>	
<i>Curtis L. Todd, Atlanta Metropolitan State College, USA</i>	
Hactivism and Alternative Journalism: The Case of the French YouTube Channel Thinkerview ...	347
<i>Christophe Emmanuel Premat, Stockholm University, Sweden</i>	
Drifting on the Web	362
<i>Lila Luchessi, Universidad Nacional de Río Negro, Argentina & Universidad de Buenos Aires, Argentina</i>	
<i>Ana Lambrecht, Universidad Nacional de Río Negro, Argentina</i>	

Volume II

Cyber Crime Regulation, Challenges, and Response	374
<i>Sachin Tiwari, Jawaharlal Nehru University, India</i>	

Regulating the Internet.....	392
<i>David T. A. Wesley, Northeastern University, USA</i>	
Cybersecurity Legislation	402
<i>Christopher Thomas Anglim, University of the District of Columbia, USA</i>	
International Context of Cybercrime and Cyber Law.....	412
<i>Tansif Ur Rehman, University of Karachi, Pakistan</i>	
International Cooperation and Legal Response to Cybercrime in Pakistan	424
<i>Tansif Ur Rehman, University of Karachi, Pakistan</i>	
Cybersecurity Laws in Malaysia	435
<i>Olivia Swee Leng Tan, Multimedia University, Malaysia</i>	
<i>Rossanne Gale Vergara, Multimedia University, Malaysia</i>	
<i>Raphael C. W. Phan, Multimedia University, Malaysia</i>	
<i>Shereen Khan, Multimedia University, Malaysia</i>	
<i>Nasreen Khan, Multimedia University, Malaysia</i>	
Game Console Protection and Breaking It.....	449
<i>Nezer Jacob Zaidenberg, College of Management, Israel</i>	

Section 3: Drug Trafficking, Human Trafficking, and the Sexual Exploitation of Children

Drug Trafficking.....	463
<i>Prabhjyot Kaur, University of Delhi, India</i>	
<i>Puneet Kumar Kaushal, Lucideus Technologies, India</i>	
Domain-Specific Search Engines for Investigating Human Trafficking and Other Illicit Activities ..	478
<i>Mayank Kejriwal, University of Southern California, USA</i>	
Identifying Victims of Human Sex Trafficking in Online Ads	497
<i>Jessica Whitney, San Diego State University, USA</i>	
<i>Marisa Hultgren, San Diego State University, USA</i>	
<i>Murray Eugene Jennex, San Diego State University, USA</i>	
<i>Aaron Elkins, San Diego State University, USA</i>	
<i>Eric Frost, San Diego State University, USA</i>	
Human Trafficking and Cyber Laws in Malaysia.....	518
<i>Olivia Swee Leng Tan, Multimedia University, Malaysia</i>	
<i>Rossanne Gale Vergara, Multimedia University, Malaysia</i>	
<i>Raphael C. W. Phan, Multimedia University, Malaysia</i>	
<i>Shereen Khan, Multimedia University, Malaysia</i>	
<i>Nasreen Khan, Multimedia University, Malaysia</i>	

Web-Based Child Sexual Exploitation.....	533
<i>Lacey Nicole Wallace, Penn State Altoona, USA</i>	
Using Luring Communication Theory to Analyze the Behavior of Online Sexual Offenders	547
<i>Charles R. Crowell, University of Notre Dame, USA</i>	
<i>Jamie Segerson, University of Notre Dame, USA</i>	
<i>Mitchell D. Kajzer, University of Notre Dame, USA</i>	
<i>Michael Villano, University of Notre Dame, USA</i>	
<i>Julaine Zenk, University of Notre Dame, USA</i>	
<i>Veronica Wegner, University of Notre Dame, USA</i>	
<i>Monica M. Bell, University of Notre Dame, USA</i>	
ICTs and Sexual Exploitation of Children in Europe	565
<i>László Dornfeld, Ferenc Mádl Institute of Comparative Law, Hungary</i>	
Regulating Misandry: Expanding the Protection Against Online Hate Speech.....	580
<i>Maria Mpasdeki, NGO Solidarity Now, Athens, Greece</i>	
<i>Zafeiris Tsiftzis, University of Bolton, UK</i>	
Online Hate Crimes Against Women (CYBER VAWG)	591
<i>Tehmina Khan, RMIT University, Australia</i>	
Intimate Partner Cyber Abuse Viewed Through the Lens of Criminology	606
<i>Curtis L. Todd, Atlanta Metropolitan State College, USA</i>	
<i>Joshua E. Byrd, American Intercontinental University, USA</i>	
<i>Leroy Baldwin, Atlanta Metropolitan State College, USA</i>	
The Dark Side of Engaging With Social Networking Sites (SNS).....	615
<i>Eileen O'Donnell, Technological University Dublin, Ireland</i>	
<i>Liam O'Donnell, Technological University Dublin, Ireland</i>	
Cyberstalking: The New Threat on the Internet	628
<i>Edith Huber, Danube University Krems, Austria</i>	
<i>Roman H. Brandtweiner, Vienna University of Economics and Business, Austria</i>	
The Nature of Cyberbullying Among Youths.....	640
<i>Michelle F. Wright, Penn State University, USA</i>	
Internet “Death Groups” in the Online Culture	660
<i>Liudmila Vladimirovna Baeva, Astrakhan State University, Russia</i>	
Tech That, Bully! Defeating Cyberbullying With Its Own Weapons	668
<i>Maria Rosa Miccoli, Idego Psicologia Digitale, Italy</i>	
<i>Giulia Gargaglione, Idego Psicologia Digitale, Italy</i>	
<i>Simone Barbato, Idego Psicologia Digitale, Italy</i>	
<i>Lorenzo Di Natale, Idego Psicologia Digitale, Italy</i>	

Valentina Rotelli, *Idego Psicologia Digitale, Italy*
Valentina Silvestri, *University of Milan-Bicocca, Italy*

Cyberbullying in the Workplace	686
<i>Shalini Ramdeo, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
<i>Riann Singh, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
Cyber Crime Against Women and Girls on Social Sites in Bangladesh.....	699
<i>Fardaus Ara, Rajshahi University, Bangladesh</i>	

Section 4: Financial Fraud, Identity Theft, and Social Manipulation Through Social Media

Internet Privacy	715
<i>Nathan John Rodriguez, Weber State University, USA</i>	
Societal Safety and Preservation in the Digital Era	732
<i>Dylas Gudoshava, Zimbabwe Open University, Zimbabwe</i>	
Privacy and Security Challenges in the Internet of Things	749
<i>Fernando Almeida, Polytechnic Institute of Gaya, Portugal</i>	
<i>Justino Lourenço, Polytechnic Institute of Gaya, Portugal</i>	

Volume III

Cybercrime and Private Health Data: Review, Current Developments, and Future Trends	763
<i>Stavros Pitoglou, National Technical University of Athens, Greece & Computer Solutions SA, Greece</i>	
<i>Dimitra Giannouli, Computer Solutions SA, Greece & University of Leeds, UK</i>	
<i>Vassilia Costarides, Institute of Communication and Computer Systems (ICCS), Greece</i>	
<i>Thelma Androutsou, National Technical University of Athens, Greece</i>	
<i>Athanasios Anastasiou, National Technical University of Athens, Greece</i>	
The Emerging Threats of Web Scrapping to Web Applications Security and Their Defense Mechanism	788
<i>Rizwan Ur Rahman, Maulana Azad National Institute of Technology, Bhopal, India</i>	
<i>Danish Wadhwa, JayPee University of Information Technology, Solan, India</i>	
<i>Aakash Bali, JayPee University of Information Technology, Solan, India</i>	
<i>Deepak Singh Tomar, Maulana Azad National Institute of Technology, Bhopal, India</i>	
Social Engineering Using Social Networking Sites.....	810
<i>Roberto Marmo, University of Pavia, Italy</i>	

Social Media and Identity Theft Implications on Nigerian Victims and International Economy	823
<i>Tolulope Kayode-Adedeji, Covenant University, Nigeria</i>	
<i>Obianuju Victoria Okeke, Covenant University, Nigeria</i>	
<i>Lanre Amodu, Covenant University, Nigeria</i>	
<i>Opeyemi Fasanya, Covenant University, Nigeria</i>	
<i>Nelson Okorie, Covenant University, Nigeria</i>	
Online Phishing and Solutions.....	837
<i>Ping Wang, Robert Morris University, USA</i>	
<i>Anteneh T. Girma, University of District of Columbia, USA</i>	
Crime Hidden in Email Spam.....	851
<i>Szde Yu, Wichita State University, USA</i>	
Classification of Spamming Attacks to Blogging Websites and Their Security Techniques.....	864
<i>Rizwan Ur Rahman, Maulana Azad National Institute of Technology, Bhopal, India</i>	
<i>Rishu Verma, Jaypee University of Information Technology, India</i>	
<i>Himani Bansal, Jaypee University, Solan, India</i>	
<i>Deepak Singh Tomar, Maulana Azad National Institute of Technology, Bhopal, India</i>	
Cybercrime in Online Gaming.....	881
<i>Boaventura DaCosta, Solers Research Group, USA</i>	
<i>Soonhwa Seok, Korea University, South Korea</i>	
E-Banking Security: Threats, Challenges, Solutions, and Trends	893
<i>Fabio Diniz Rossi, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
<i>Rumenigüe Hohemberger, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
<i>Marcos Paulo Konzen, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
<i>Daniel Chaves Temp, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
E-Banking Frauds: The Current Scenario and Security Techniques	905
<i>Sandal Azhar, University of Delhi, India</i>	
<i>Manisha Shahi, University of Delhi, India</i>	
<i>Vikas Chhapola, University of Delhi, India</i>	
Tackle the Smart Contract Vulnerabilities	919
<i>Parthasarathi R., Delhi University, India</i>	
<i>Puneet Kaushal, Lucideus Technologies, India</i>	
The Challenges and Future of E-Wallet	932
<i>Chiam Chooi Chea, Open University Malaysia, Malaysia</i>	

Preliminary Insights Into the Adoption of Bitcoin in a Developing Economy: The Case of Ghana..	945
<i>Frederick Edem Broni, University of Ghana Business School, Ghana</i>	
<i>Richard Boateng, University of Ghana Business School, Ghana</i>	
<i>Acheampong Owusu, University of Ghana Business School, Ghana</i>	

Section 5: Security Tools and Solutions, Human-Based Cyber Defense, and the Social Understanding of Threats

The Importance of the Human-Centric Approach in Combating Cyber Threats	965
<i>Pamela Goh, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>Loo Seng Neo, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>Xingyu Chen, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
Understanding the Relationship Between Cybercrime and Human Behavior Through Criminological Theories and Social Networking Sites.....	979
<i>Anne-Marie Mohammed, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
<i>Vladlena Benson, Aston Business School, UK</i>	
<i>George Saridakis, University of Kent, UK</i>	
Online Expression, Personal Cybersecurity Costs, and the Specter of Cybercrime.....	990
<i>Juhani Rauhala, University of Jyväskylä, Finland</i>	
<i>Pasi Tyrväinen, University of Jyväskylä, Finland</i>	
<i>Nezer Zaidenberg, College of Management Academic Studies, Israel</i>	
Leveraging on Digital Footprints to Identify Potential Security Threats: Insights From the Behavioural Sciences Perspective.....	1003
<i>Loo Seng Neo, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
Investigating Cybercrime in Nigeria.....	1018
<i>Mufutau Temitayo Lamidi, University of Ibadan, Nigeria</i>	
Machine Learning and Cyber Security: Future Potential of the Research.....	1034
<i>Vardan Mkrttchian, HHH University, Australia</i>	
<i>Sergey Kanarev, Penza State University, Russia</i>	
<i>Leyla Gamidullaeva, Penza State University, Russia</i>	
Perspective Tools to Improve Machine Learning Applications for Cyber Security	1043
<i>Vardan Mkrttchian, HHH University, Australia</i>	
<i>Leyla Gamidullaeva, Penza State University, Russia</i>	

An Overview (and Criticism) of Methods to Detect Fake Content Online	1053
<i>Antonio Badia, University of Louisville, USA</i>	
Crookies: Tampering With Cookies to Defraud E-Marketing	1062
<i>Bede Ravindra Amarasekara, Massey University, New Zealand</i>	
<i>Anuradha Mathrani, Massey University, New Zealand</i>	
<i>Chris Scogings, Massey University, New Zealand</i>	
Crime Identification Using Traffic Analysis of HTTP Botnet	1077
<i>Ciza Thomas, Directorate of Technical Education, India</i>	
Hybrid Artificially Intelligent Multi-Layer Blockchain and Bitcoin Cryptology (AI-MLBBC): Anti-Crime-Theft Smart Wall Defense	1089
<i>Murad Al Shibli, Abu Dhabi Polytechnic, UAE</i>	
An IBE-Based Authenticated Key Transfer Protocol on Elliptic Curves	1112
<i>Daya Sagar Gupta, Shershah College of Engineering Sasaram Bihar, India</i>	
Efficiency Issues and Improving Implementation of Keystroke Biometric Systems	1123
<i>Ali Kartit, LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco</i>	
<i>Farida Jaha, LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco</i>	
Modern Blue Pills and Red Pills	1136
<i>Asaf Algawi, University of Jyväskylä, Finland</i>	
<i>Michael Kiperberg, Holon Institute of Technology, Israel</i>	
<i>Roe Shimon Leon, University of Jyväskylä, Finland</i>	
<i>Amit Resh, Shenkar College, Israel</i>	
<i>Nezer Jacob Zaidenberg, College of Management, Israel</i>	
Arm Hypervisor and Trustzone Alternatives	1150
<i>Nezer Jacob Zaidenberg, College of Management, Israel</i>	
<i>Raz Ben Yehuda, University of Jyväskylä, Finland</i>	
<i>Roe Leon, University of Jyväskylä, Finland</i>	
Glossary	xxxvi
Compilation of References	lxiii
About the Contributors	ccviii
Index	ccxxxiii

Alphabetical Table of Contents

Academic Integrity of Global Digital Masked Bandits Lurking the Deep and Dark Web	177
<i>David B. Ross, Nova Southeastern University, USA</i>	
<i>Julie A. Exposito, Nova Southeastern University, USA</i>	
<i>Melissa T. Sasso, Nova Southeastern University, USA</i>	
<i>Cortney E. Matteson, Orange County School District, USA</i>	
<i>Rande W. Matteson, Nova Southeastern University, USA</i>	
Arm Hypervisor and Trustzone Alternatives.....	1150
<i>Nezer Jacob Zaidenberg, College of Management, Israel</i>	
<i>Raz Ben Yehuda, University of Jyväskylä, Finland</i>	
<i>Roe Leon, University of Jyväskylä, Finland</i>	
Artificial Intelligence-Based Cybercrime	36
<i>Bogdan Hoanca, University of Alaska, Anchorage, USA</i>	
<i>Kenrick J. Mock, University of Alaska, Anchorage, USA</i>	
The Challenges and Future of E-Wallet	932
<i>Chiam Chooi Chea, Open University Malaysia, Malaysia</i>	
Classification of Spamming Attacks to Blogging Websites and Their Security Techniques.....	864
<i>Rizwan Ur Rahman, Maulana Azad National Institute of Technology, Bhopal, India</i>	
<i>Rishu Verma, Jaypee University of Information Technology, India</i>	
<i>Himani Bansal, Jaypee University, Solan, India</i>	
<i>Deepak Singh Tomar, Maulana Azad National Institute of Technology, Bhopal, India</i>	
Crime Hidden in Email Spam	851
<i>Szde Yu, Wichita State University, USA</i>	
Crime Identification Using Traffic Analysis of HTTP Botnet	1077
<i>Ciza Thomas, Directorate of Technical Education, India</i>	

Crime-Fake News Nexus	52
<i>Xingyu Chen, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>John Yu, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>Pamela Goh, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>Loo Seng Neo, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>Verity Er, Home Team Behavioural Sciences, Ministry of Home Affairs, Singapore</i>	
<i>Majeed Khader, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
Crookies: Tampering With Cookies to Defraud E-Marketing.....	1062
<i>Bede Ravindra Amarasekara, Massey University, New Zealand</i>	
<i>Anuradha Mathrani, Massey University, New Zealand</i>	
<i>Chris Scogings, Massey University, New Zealand</i>	
Cyber Crime Against Women and Girls on Social Sites in Bangladesh.....	699
<i>Fardaus Ara, Rajshahi University, Bangladesh</i>	
Cyber Crime Regulation, Challenges, and Response	374
<i>Sachin Tiwari, Jawaharlal Nehru University, India</i>	
Cyberbullying in the Workplace	686
<i>Shalini Ramdeo, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
<i>Riann Singh, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
Cybercrime.....	1
<i>Poongodi Thangamuthu, Galgotias University, India</i>	
<i>Anu Rathee, Maharaja Agrasen Institute of Technology, India</i>	
<i>Suresh Palanimuthu, Galgotias University, India</i>	
<i>Balamurugan Balusamy, Galgotias University, India</i>	
Cybercrime and Private Health Data: Review, Current Developments, and Future Trends.....	763
<i>Stavros Pitoglou, National Technical University of Athens, Greece & Computer Solutions SA, Greece</i>	
<i>Dimitra Giannouli, Computer Solutions SA, Greece & University of Leeds, UK</i>	
<i>Vassilia Costarides, Institute of Communication and Computer Systems (ICCS), Greece</i>	
<i>Thelma Androutsou, National Technical University of Athens, Greece</i>	
<i>Athanasios Anastasiou, National Technical University of Athens, Greece</i>	
Cybercrime in Online Gaming.....	881
<i>Boaventura DaCosta, Solers Research Group, USA</i>	
<i>Soonhwa Seok, Korea University, South Korea</i>	

Cybersecurity Laws in Malaysia	435
<i>Olivia Swee Leng Tan, Multimedia University, Malaysia</i>	
<i>Rossanne Gale Vergara, Multimedia University, Malaysia</i>	
<i>Raphael C. W. Phan, Multimedia University, Malaysia</i>	
<i>Shereen Khan, Multimedia University, Malaysia</i>	
<i>Nasreen Khan, Multimedia University, Malaysia</i>	
Cybersecurity Legislation	402
<i>Christopher Thomas Anglim, University of the District of Columbia, USA</i>	
Cyberstalking: The New Threat on the Internet	628
<i>Edith Huber, Danube University Krems, Austria</i>	
<i>Roman H. Brandtweiner, Vienna University of Economics and Business, Austria</i>	
The Dark Side of Engaging With Social Networking Sites (SNS)	615
<i>Eileen O'Donnell, Technological University Dublin, Ireland</i>	
<i>Liam O'Donnell, Technological University Dublin, Ireland</i>	
The Dark Web: Hidden Access to Internet Today	129
<i>Ramanujam Elangovan, Thiagarajar College of Engineering, India</i>	
Dark Web: A Boon or a Bane	152
<i>Punam Bedi, University of Delhi, India</i>	
<i>Neha Gupta, University of Delhi, India</i>	
<i>Vinita Jindal, Keshav Mahavidyalaya, University of Delhi, India</i>	
Developing Cyber Buffer Zones	287
<i>Michael Robinson, Airbus, UK</i>	
<i>Kevin Jones, Airbus, UK</i>	
<i>Helge Janicke, De Montfort University, UK</i>	
<i>Leandros Maglaras, De Montfort University, UK</i>	
Development of Crime Sociology From Bureaucratic Iron Cage to Digital Determination	229
<i>Muhammet Ali Köroğlu, Uşak University, Turkey</i>	
Domain-Specific Search Engines for Investigating Human Trafficking and Other Illicit Activities ..	478
<i>Mayank Kejriwal, University of Southern California, USA</i>	
Drifting on the Web	362
<i>Lila Luchessi, Universidad Nacional de Río Negro, Argentina & Universidad de Buenos Aires, Argentina</i>	
<i>Ana Lambrecht, Universidad Nacional de Río Negro, Argentina</i>	

Drug Trafficking.....	463
<i>Prabhjyot Kaur, University of Delhi, India</i>	
<i>Puneet Kumar Kaushal, Lucideus Technologies, India</i>	
E-Banking Frauds: The Current Scenario and Security Techniques	905
<i>Sandal Azhar, University of Delhi, India</i>	
<i>Manisha Shahi, University of Delhi, India</i>	
<i>Vikas Chhapola, University of Delhi, India</i>	
E-Banking Security: Threats, Challenges, Solutions, and Trends	893
<i>Fabio Diniz Rossi, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
<i>Rumenigüe Hohemberger, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
<i>Marcos Paulo Konzen, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
<i>Daniel Chaves Temp, Federal Institute of Education, Science, and Technology of Farroupilha, Brazil</i>	
Efficiency Issues and Improving Implementation of Keystroke Biometric Systems.....	1123
<i>Ali Kartit, LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco</i>	
<i>Farida Jaha, LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco</i>	
The Emerging Threats of Web Scrapping to Web Applications Security and Their Defense Mechanism.....	788
<i>Rizwan Ur Rahman, Maulana Azad National Institute of Technology, Bhopal, India</i>	
<i>Danish Wadhwa, JayPee University of Information Technology, Solan, India</i>	
<i>Aakash Bali, JayPee University of Information Technology, Solan, India</i>	
<i>Deepak Singh Tomar, Maulana Azad National Institute of Technology, Bhopal, India</i>	
File-Sharing and the Darknet.....	165
<i>Martin Steinebach, Fraunhofer SIT, Germany</i>	
Game Console Protection and Breaking It.....	449
<i>Nezer Jacob Zaidenberg, College of Management, Israel</i>	
The Globalization of Hybrid Warfare and the Need for Plausible Deniability.....	242
<i>Benedict E. DeDominicis, Catholic University of Korea, South Korea</i>	
Grey Zone Conflicts in Cyber Domain: Nonlocality of Political Reality in the World of “Hyperobjects”	271
<i>Muhammed Can, University of Minho, Portugal</i>	

Hactivism and Alternative Journalism: The Case of the French YouTube Channel Thinkerview ...	347
<i>Christophe Emmanuel Premat, Stockholm University, Sweden</i>	
Human Trafficking and Cyber Laws in Malaysia.....	518
<i>Olivia Swee Leng Tan, Multimedia University, Malaysia</i>	
<i>Rossanne Gale Vergara, Multimedia University, Malaysia</i>	
<i>Raphael C. W. Phan, Multimedia University, Malaysia</i>	
<i>Shereen Khan, Multimedia University, Malaysia</i>	
<i>Nasreen Khan, Multimedia University, Malaysia</i>	
Hybrid Artificially Intelligent Multi-Layer Blockchain and Bitcoin Cryptology (AI-MLBBC): Anti-Crime-Theft Smart Wall Defense	1089
<i>Murad Al Shibli, Abu Dhabi Polytechnic, UAE</i>	
An IBE-Based Authenticated Key Transfer Protocol on Elliptic Curves	1112
<i>Daya Sagar Gupta, Shershah College of Engineering Sasaram Bihar, India</i>	
ICTs and Sexual Exploitation of Children in Europe	565
<i>László Dornfeld, Ferenc Mádl Institute of Comparative Law, Hungary</i>	
Identifying Victims of Human Sex Trafficking in Online Ads	497
<i>Jessica Whitney, San Diego State University, USA</i>	
<i>Marisa Hultgren, San Diego State University, USA</i>	
<i>Murray Eugene Jennex, San Diego State University, USA</i>	
<i>Aaron Elkins, San Diego State University, USA</i>	
<i>Eric Frost, San Diego State University, USA</i>	
The Importance of the Human-Centric Approach in Combating Cyber Threats	965
<i>Pamela Goh, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>Loo Seng Neo, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
<i>Xingyu Chen, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
International Context of Cybercrime and Cyber Law.....	412
<i>Tansif Ur Rehman, University of Karachi, Pakistan</i>	
International Cooperation and Legal Response to Cybercrime in Pakistan	424
<i>Tansif Ur Rehman, University of Karachi, Pakistan</i>	
Internet “Death Groups” in the Online Culture	660
<i>Liudmila Vladimirovna Baeva, Astrakhan State University, Russia</i>	

Internet Privacy	715
<i>Nathan John Rodriguez, Weber State University, USA</i>	
Intimate Partner Cyber Abuse Viewed Through the Lens of Criminology	606
<i>Curtis L. Todd, Atlanta Metropolitan State College, USA</i>	
<i>Joshua E. Byrd, American Intercontinental University, USA</i>	
<i>Leroy Baldwin, Atlanta Metropolitan State College, USA</i>	
Investigating Cybercrime in Nigeria.....	1018
<i>Mufutau Temitayo Lamidi, University of Ibadan, Nigeria</i>	
Left-Wing Extremism From the Indian Perspective: An Econometric Interpretation	93
<i>Sovik Mukherjee, St. Xavier's University, Kolkata, India</i>	
Leveraging on Digital Footprints to Identify Potential Security Threats: Insights From the Behavioural Sciences Perspective.....	1003
<i>Loo Seng Neo, Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore</i>	
Machine Learning and Cyber Security: Future Potential of the Research.....	1034
<i>Vardan Mkrtchian, HHH University, Australia</i>	
<i>Sergey Kanarev, Penza State University, Russia</i>	
<i>Leyla Gamidullaeva, Penza State University, Russia</i>	
The Management of Whistleblowing.....	304
<i>Riann Singh, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
<i>Shalini Ramdeo, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
Modern Blue Pills and Red Pills.....	1136
<i>Asaf Algawi, University of Jyväskylä, Finland</i>	
<i>Michael Kiperberg, Holon Institute of Technology, Israel</i>	
<i>Roe Shimon Leon, University of Jyväskylä, Finland</i>	
<i>Amit Resh, Shenkar College, Israel</i>	
<i>Nezer Jacob Zaidenberg, College of Management, Israel</i>	
Modus Operandi in Cybercrime	193
<i>Bettina Pospisil, Danube University Krems, Austria</i>	
<i>Edith Huber, Danube University Krems, Austria</i>	
<i>Gerald Quirchmayr, University of Vienna, Austria</i>	
<i>Walter Seboeck, Danube University Krems, Austria</i>	
The Nature of Cyberbullying Among Youths.....	640
<i>Michelle F. Wright, Penn State University, USA</i>	

Necessity of Paradigm Shift in Criminological Theorizing.....	210
<i>Ajibade Ebenezer Jegede, Covenant University, Nigeria</i>	
<i>Olusola Oyero, Covenant University, Nigeria</i>	
<i>Nelson Okorie, Covenant University, Nigeria</i>	
<i>Caleb Abiodun Ayedun, Covenant University, Nigeria</i>	
<i>Mofoluwake Ajayi, Covenant University, Nigeria</i>	
Online Activism to Cybercrime.....	334
<i>Anita W. McMurtry, Atlanta Metropolitan State College, USA</i>	
<i>Larry D. Stewart, Atlanta Metropolitan State College, USA</i>	
<i>Curtis L. Todd, Atlanta Metropolitan State College, USA</i>	
Online Expression, Personal Cybersecurity Costs, and the Specter of Cybercrime.....	990
<i>Juhani Rauhala, University of Jyväskylä, Finland</i>	
<i>Pasi Tyrväinen, University of Jyväskylä, Finland</i>	
<i>Nezer Zaidenberg, College of Management Academic Studies, Israel</i>	
Online Hate Crimes Against Women (CYBER VAWG)	591
<i>Tehmina Khan, RMIT University, Australia</i>	
Online Phishing and Solutions.....	837
<i>Ping Wang, Robert Morris University, USA</i>	
<i>Anteneh T. Girma, University of District of Columbia, USA</i>	
An Overview (and Criticism) of Methods to Detect Fake Content Online	1053
<i>Antonio Badia, University of Louisville, USA</i>	
Perspective Tools to Improve Machine Learning Applications for Cyber Security	1043
<i>Vardan Mkrttchian, HHH University, Australia</i>	
<i>Leyla Gamidullaeva, Penza State University, Russia</i>	
Preliminary Insights Into the Adoption of Bitcoin in a Developing Economy: The Case of Ghana..	945
<i>Frederick Edem Broni, University of Ghana Business School, Ghana</i>	
<i>Richard Boateng, University of Ghana Business School, Ghana</i>	
<i>Acheampong Owusu, University of Ghana Business School, Ghana</i>	
Privacy and Security Challenges in the Internet of Things	749
<i>Fernando Almeida, Polytechnic Institute of Gaya, Portugal</i>	
<i>Justino Lourenço, Polytechnic Institute of Gaya, Portugal</i>	
Privacy, Ethics, and the Dark Web.....	140
<i>Richard T. Herschel, Saint Joseph's University, USA</i>	

Regulating Misandry: Expanding the Protection Against Online Hate Speech.....	580
<i>Maria Mpasdeki, NGO Solidarity Now, Athens, Greece</i>	
<i>Zafeiris Tsiftzis, University of Bolton, UK</i>	
Regulating the Internet.....	392
<i>David T. A. Wesley, Northeastern University, USA</i>	
Social Engineering Using Social Networking Sites.....	810
<i>Roberto Marmo, University of Pavia, Italy</i>	
Social Media and Identity Theft Implications on Nigerian Victims and International Economy	823
<i>Tolulope Kayode-Adedeji, Covenant University, Nigeria</i>	
<i>Obianuju Victoria Okeke, Covenant University, Nigeria</i>	
<i>Lanre Amodu, Covenant University, Nigeria</i>	
<i>Opeyemi Fasanya, Covenant University, Nigeria</i>	
<i>Nelson Okorie, Covenant University, Nigeria</i>	
Societal Safety and Preservation in the Digital Era	732
<i>Dylas Gudoshava, Zimbabwe Open University, Zimbabwe</i>	
The Spy Who Never Has to Go Out Into the Cold Cyber Espionage	258
<i>Laura Pinto Hansen, Western New England University, USA</i>	
A Survey on Emerging Cyber Crimes and Their Impact Worldwide	23
<i>Suraj Gangwar, University of Delhi, India</i>	
<i>Vinayak Narang, University of Delhi, India</i>	
Tackle the Smart Contract Vulnerabilities	919
<i>Parthasarathi R., Delhi University, India</i>	
<i>Puneet Kaushal, Lucideus Technologies, India</i>	
Tech That, Bully! Defeating Cyberbullying With Its Own Weapons	668
<i>Maria Rosa Miccoli, Idego Psicologia Digitale, Italy</i>	
<i>Giulia Gargaglione, Idego Psicologia Digitale, Italy</i>	
<i>Simone Barbato, Idego Psicologia Digitale, Italy</i>	
<i>Lorenzo Di Natale, Idego Psicologia Digitale, Italy</i>	
<i>Valentina Rotelli, Idego Psicologia Digitale, Italy</i>	
<i>Valentina Silvestri, University of Milan-Bicocca, Italy</i>	
Transnational Cybercrime: The Dark Web	108
<i>Barbara Jane Holland, Brooklyn Public Library, USA</i>	

Understanding the Relationship Between Cybercrime and Human Behavior Through Criminological Theories and Social Networking Sites.....	979
<i>Anne-Marie Mohammed, The University of the West Indies, St. Augustine, Trinidad and Tobago</i>	
<i>Vladlena Benson, Aston Business School, UK</i>	
<i>George Saridakis, University of Kent, UK</i>	
Unveiling Cybercrime in a Developing Country	66
<i>Richard Boateng, University of Ghana Business School, Ghana</i>	
<i>Jonathan Nii Barnor Barnor, University of Ghana Business School, Ghana</i>	
Using Luring Communication Theory to Analyze the Behavior of Online Sexual Offenders	547
<i>Charles R. Crowell, University of Notre Dame, USA</i>	
<i>Jamie Segerson, University of Notre Dame, USA</i>	
<i>Mitchell D. Kajzer, University of Notre Dame, USA</i>	
<i>Michael Villano, University of Notre Dame, USA</i>	
<i>Julaine Zenk, University of Notre Dame, USA</i>	
<i>Veronica Wegner, University of Notre Dame, USA</i>	
<i>Monica M. Bell, University of Notre Dame, USA</i>	
Web-Based Child Sexual Exploitation.....	533
<i>Lacey Nicole Wallace, Penn State Altoona, USA</i>	
Whistleblowing to Expose Criminal Activity in the Health Sector	318
<i>Niyi Awofeso, School of Health and Environmental Studies, Hamdan Bin Mohammed Smart University, UAE</i>	

Preface

Technological advancements of the past few decades, particularly those related to the world wide web, have provided new platforms and outlets for criminals to conduct unlawful and unethical behavior. Sadly, these criminals have identified ways to both use and exploit this technology for devious means, ranging from data breaches, theft, cyberstalking, embezzlement, human trafficking, child abuse, to many other cunning actions that are impacting individuals, corporations, and government entities all over the world. These days, innocent law-abiding citizens are under constant attack by these cybercriminals and it's drastically affecting every aspect of their daily life, whether they are aware of it or not.

Over time, individuals, governments, law enforcement agencies, and businesses have been advancing their data harvesting, tracking, and management techniques to collect information about web users and their online activities with the hope of better understanding their digital footprints. While they mean no harm and are merely trying to more efficiently target their efforts and increase their overall data integrity, the reality is that there are millions of cybercriminals out there who have much more devious intentions in mind and are using these practices to gather private data information about individuals and organizational entities for exploitative purposes.

Even with the web being prevalent for decades now, most still do not understand that there is no real privacy online, and as such so much information about individuals and groups is continually being shared out either publicly or within personal accounts and online groups. Criminals are just waiting for the opportune moment to seize information from these so-called trusted environments as they now have access to hidden portions of the world wide web, better known as the “deep web”, where they can freely access and share private information about everyone and everything.

While the deep web consists of sites that simply cannot be found through traditional search engines, the “dark web” emerged as a portion of the world wide web that was intentionally hidden, operating under extreme secrecy and inaccessible through standard browsers. Criminals can navigate through these sites anonymously, leaving no trackable digital information behind. The deep web has become an ideal source of information for criminals engaging in a range of illegal activities such as human trafficking, child exploitation, murder, and selling social security numbers, drugs, and many more illegal goods and services.

Although most individuals around the world are not very familiar with the existence of the deep web and do not know how the deep web can affect them and their personal privacy, these sites present significant threats to all people and organizations worldwide. Regrettably, the primary source of information that is available on the deep web and utilized by these criminals happens to be provided freely and willingly by all those uninformed individuals and organizations that post personal and proprietary

information across social media and other online channels. They do not realize that by sharing information such as their birth date, their home address, and pictures of themselves and of their loved ones, that they are putting themselves and others at risk.

This seemingly private information can be easily accessed by cybercriminals which is then shared through the deep web all over the world. Cybercriminals worldwide can be very technology savvy and highly intelligent individuals who can hack bank accounts, social media accounts, websites, private networks, etc. and in many cases can easily persuade average users to reveal confidential information through fraudulent e-mail messages known as phishing attacks. They can stalk and harass their victims online and through gaming platforms, sometimes even using these mediums to lure them to a physical meeting place where they can kidnap, assault, or kill their victims. Regrettably, many minors and children are the primary victims of these luring criminal schemes.

On an even larger scale, the deep web also threatens many organizations, businesses, governments and their thousands, millions, or even billions of employees, customers, and citizens globally. These entities can be subject to cyberattacks, that can lead to credit theft, embezzlement, service disruption, the stealing of trade secrets, the sharing of confidential information, and in some cases the use of a denial-of-service (DoS) attack for ransoms. These activities also have significant implications on governments as they provide the anonymity ideal for spying on each other and provides individuals with the opportunity to sell government secrets with less risk, and in some cases even having the ability to rig democratic processes and elections. Ironically, the deep web also provides the concealment necessary for hacktivists to illegally reveal the personal information of the individuals that are committing such illicit activities.

As the deep web become more widely known as a primary source of illegal goods and services offered by criminals, there are calls for government regulations and policies to be put in place, leading to controversial discussions as to whether one country's government can place restrictions on an international tool and whether de-anonymizing the dark web is an infringement on individual rights. Currently, in most western societies, internet access and data privacy remain a heated issue with government officials attempting to navigate new policies that will better secure their citizens' online information. Many governments and their laws have not kept pace with the rapid increase in the use of the deep web for criminal activities, which is providing cybercriminals fertile ground for committing such actions. Although government policies and laws are extremely essential in dealing with these problems, the best way to truly deal with these threats that the deep web poses is through knowledge transmission, as the public needs to become much more knowledgeable and aware of these realities and ways that they can protect themselves.

Academics and researchers play a significant role in assisting the general public with learning more about these phenomena and ways to deal with them. As cybercriminals develop more advanced strategies to expand their criminal enterprise, society needs to become much more knowledgeable and educated about ways to combat these threats and cyberattacks that are costing many people and organizations around the world tremendous pain, anguish, discomfort, and billions of dollars in damages. Users of the world wide web can become collectively much more aware of protecting themselves and denying criminals access to private and personal information.

To facilitate the knowledge development process and provide the latest research discoveries on this relevant topic, the *Encyclopedia of Criminal Activities and the Deep Web* is a three-volume compilation that showcases recent findings, trends, challenges, and solutions brought forth by hundreds of promi-

ment researchers and experts from all over the world. With 79 individual article contributions containing very thorough coverage of all aspects of criminal activities related to the world wide web and the various challenges they pose to all societies and their citizens and organizations, this comprehensive encyclopedia substantially contributes to the body of literature surrounding the controversial use of the dark and deep web.

This publication serves as an excellent source for the latest discoveries in this area and will benefit criminologists, forensic scientists, sociologists, journalists, victim advocates, academicians, researchers, and students who are looking to gain further knowledge about cybercriminals and the deep web, and will empower law enforcement agencies, government officials, and policy and law makers to enact solutions for the protection of society. Furthermore, information technology specialists, cybersecurity analysts, data scientists, and other industry professionals will also greatly benefit from this extensive research which will ideally inspire new methods of data security and protection.

The *Encyclopedia of Criminal Activities and the Deep Web* is designed to act as a sole reference source on conceptual, methodological, and technical aspects, and will provide an understanding of emerging topics including, but not limited to: cyber harassment, internet privacy, cyber espionage, darknet, social engineering, online gaming, online phishing, social networking, hacktivism, and cyber law. The article manuscripts included in this publication have all been subjected to a double-blind peer review process and have satisfied all review requirements and were accepted by the reviewers of this publication. The contents of this publication are certain to provide readers the necessary means for further research and innovation in their relevant area of research related to the theme of this publication.

The *Encyclopedia of Criminal Activities and the Deep Web* is organized into five separate sections that provide comprehensive coverage of critical topics. The sections are:

1. Cybercriminal Profiles, Understanding Cybercrime, and the Realities of the Dark Web;
2. Cyberwarfare, Cybersecurity, Spyware, and Regulatory Policies and Solutions;
3. Drug Trafficking, Human Trafficking, and the Sexual Exploitation of Children;
4. Financial Fraud, Identity Theft, and Social Manipulation Through Social Media; and
5. Security Tools and Solutions, Human-Based Cyber Defense, and the Social Understanding of Threats.

Each of the focused sections include diverse articles centered around a common theme, with each of the articles then arranged by relevance to the theme and to each other. Two different tables of contents support the reader with navigating the contents by volume and alphabetically. Below are just a few highlighted article contributions.

SECTION 1: CYBERCRIMINAL PROFILES, UNDERSTANDING CYBERCRIME, AND THE REALITIES OF THE DARK WEB

This section provides a broad publication overview of what constitutes cybercrimes and studies into the motives behind cybercriminals. Additionally, it provides the reader with a greater understanding of the deep web and contemporary challenges posed by these sites. The first article in this section is titled “Cybercrime” and is authored by Profs. Poongodi Thangamuthu, Anu Rathee, Suresh Palanimuthu, and

Balamurugan Balusamy from Galgotias University, India. It explores the various forms of cybercrime and how they can threaten an individual or even an entire nation's security. Another article presented early within this section, "Crime-Fake News Nexus," authored by Profs. Xingyu Chen, John Yu, Pamela Goh, Loo Seng Neo, Verity Er, and Majeed Khader from Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore, examines 32 cases of fake news incidents that were perpetrated for criminal gain, which took place in Singapore from 2013 to 2018 and aims to look at the impact that these stories have had throughout Singapore. Also included in this section is the article, "Privacy, Ethics, and the Dark Web," authored by Prof. Richard T. Herschel from Saint Joseph's University, USA, which considers how companies are actively monitoring activities on the deep web as new legislation requires them to inform authorities if there has been a data breach that affects their customers. One of the closing articles, "Academic Integrity of Global Digital Masked Bandits Lurking the Deep and Dark Web," authored by Profs. David B. Ross, Julie A. Exposito, Rande W. Matteson, and Melissa T. Sasso from Nova Southeastern University, USA and Courtney E. Matteson from Orange County School District, USA, looks to enlighten teachers and administrators about the growing concern of plagiarism and deep web schemes to defraud funding sources and how they can become proactive in handling it within their own classrooms and schools. The final article within this section, "Development of Crime Sociology from Bureaucratic Iron Cage to Digital Determination," authored by Prof. Muhammet Ali Köroğlu from Uşak University, Turkey, explains how humans have always had values, norms, and rules and how these have been affected by the advent of digital technologies.

SECTION 2: CYBERWARFARE, CYBERSECURITY, SPYWARE, AND REGULATORY POLICIES AND SOLUTIONS

This section consists of content dealing with an in-depth review of cybersecurity challenges to global governments, including research on cyber espionage, whistleblowing, and hacktivism, as well as international regulations and solutions to combat and prevent online illicit activities. The first article included in this section, "The Globalization of Hybrid Warfare and the Need for Plausible Deniability," authored by Prof. Benedict E. DeDominicis from Catholic University of Korea, Korea, looks at how social media can be used as a weapon to distribute propaganda and disinformation effectively and extensively at a low or free cost and aims to strengthen surveillance capabilities to prevent its influence in significant events such as presidential elections. Another noteworthy article included in this section is "The Spy Who Never Has to Go Out Into the Cold," authored by Prof. Laura Pinto Hansen from Western New England University, USA. This article discusses how spies utilize the dark and deep web to make covert operations even more secretive and explores methods of obtaining sensitive information and disabling computer systems. Also included in this section is the article "Hacktivism and Alternative Journalism: The Case of the French YouTube Channel Thinkerview," authored by Prof. Christophe Emmanuel Premat from Stockholm University, Sweden, which explores a hacktivist YouTube channel from France and studies how the channel presents the guests and the topics to see if there is journalistic innovation. One of the closing articles in this section, "Regulating the Internet," authored by Prof. David T. A. Wesley from Northeastern University, USA, reviews the legal history of computer code as free speech in the United States and how it can be used to promote other forms of free speech through cryptography and other secure communications. It also argues that the deep and dark web are direct results of these precedents

and while they can be abused by cybercriminals and malicious state actors, they are also indispensable in promoting free speech and human rights. The last article within this section, “Game Consoles Protection and Breaking It,” authored by Prof. Nezer Jacob Zaidenberg from the College of Management, Israel, surveys attacks on various game consoles and explores the motivations behind these attacks, the way the console manufacturer acted, and the way the hacking community reacted.

SECTION 3: DRUG TRAFFICKING, HUMAN TRAFFICKING, AND THE SEXUAL EXPLOITATION OF CHILDREN

This section examines the influence of the deep web in aiding drug and human trafficking activities, as well as how it provides a protected outlet for the exploitation of children. Additionally, all forms of cyber aggression, including cyber stalking and cyberbullying are analyzed. The first article in this section, “Drug Trafficking,” authored by Prof. Prabhjyot Kaur from University of Delhi, India, and Prof. Puneet Kumar Kaushal from Lucideus Technologies, India, reviews how the deep web and dark web operate as it pertains to the sale and trade of illegal drugs online and also looks at new tactics that law enforcement are using to prevent this from happening. Another article included in this section, “Web-Based Child Sexual Exploitation,” authored by Prof. Lacey Nicole Wallace from Penn State Altoona, USA, explains online child sexual exploitation, describes the law in regards to these activities, details what is known about victims and offenders, and highlights current efforts toward prevention and intervention. Additionally included within this section is the article titled “Cyberstalking” authored by Prof. Edith Huber from Danube University Krems, Austria and Prof. Roman H. Brandtweiner from Vienna University of Economics and Business, Austria, which examines the digitalization of stalking and how it has created new crimes such as cyber harassment, cyberbullying, and other romance scams. One of the closing articles in this section, “Tech That, Bully! Defeating Cyberbullying With Its Own Weapons,” authored by Profs. Maria Rosa Miccoli, Giulia Gargaglione, and Valentina Rotelli from Catholic University of Milan, Italy; Profs. Simone Barbato and Lorenzo Di Natale from Idego - Digital Psychology Srl, Italy; and Prof. Valentina Silvestri from University of Milan - Bicocca, Italy, looks at new treatment options for cyberbullying victims including the use of a virtual reality tool which will help victims overcome their distress in a safe and protected environment. The last article within this section, “Cyber Crime Against Women and Girls on Social Sites in Bangladesh,” authored by Prof. Fardaus Ara from Rajshahi of the University of Bangladesh, Bangladesh, presents new information on cybercrimes that have been committed against women and suggests new ways to control and combat cybercrime for the future.

SECTION 4: FINANCIAL FRAUD, IDENTITY THEFT, AND SOCIAL MANIPULATION THROUGH SOCIAL MEDIA

The articles included in this section investigate challenges to internet and data privacy and the social engineering attacks that can lead to identity theft. The emergence of bitcoin and e-banking fraud are also discussed. The first article within this section, “Internet Privacy,” authored by Prof. Nathan John Rodriguez from Weber State University, USA, examines the risks of submitting personal information

online and why users may choose to exchange their personal information for a more personalized online experience. Another article included in this section, “Social Engineering Using Social Networking Sites,” authored by Prof. Roberto Marmo from University of Pavia, Italy, explains what social engineering is and it offers techniques and solutions for social engineering attacks that occur on social media websites. Another article presented in this section titled “Online Phishing and Solutions,” authored by Profs. Ping Wang and Anteneh T. Girma from Robert Morris University, USA, discusses how online phishing works to exploit human vulnerabilities and offers a comprehensive set of possible solutions to address the problem. One of the closing articles in this section, “Cybercrime in Online Gaming,” authored by Prof. Boaventura DaCosta from Solers Research Group, USA and Prof. Soonhwa Seok from Korea University, South Korea, explores cybercrimes such as data breaches, compromised and stolen data, and the theft and sale of in-game items, as it relates to the video game industry. The last article within this section, “Preliminary Insights Into the Adoption of Bitcoin in a Developing Economy,” authored by Profs. Frederick Edem Broni, Richard Boateng, and Acheampong Owusu from University of Ghana Business School, Ghana, looks at bitcoin adaptation specifically in Ghana and assesses whether or not bitcoin is preferable to other methods of payment online.

SECTION 5: SECURITY TOOLS AND SOLUTIONS, HUMAN-BASED CYBER DEFENSE, AND THE SOCIAL UNDERSTANDING OF THREATS

This section provides innovative solutions for combatting cyber threats including new technologies and tools, as well as human-based methods that can be enacted to increase awareness. The first article within this section, “The Importance of the Human-Centric Approach in Combating Cyber Threats,” authored by Profs. Pamela Goh, Loo Seng Neo, and Xingyu Chen from Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore, looks at the prevalence of cyber threats and cyberattacks and provides solutions and recommendations as to what people can do to protect themselves personally and professionally. Another article presented in this section is “Online Expression, Personal Cybersecurity Costs, and the Specter of Cybercrime,” authored by Profs. Juhani Rauhala and Pasi Tyrväinen from University of Jyväskylä, Finland and Prof. Nezer Zaidenberg from College of Management Academic Studies, Israel, examines the security and privacy risks that come with everyday internet use and also looks at what can be done to mitigate those risks in the future. Another noteworthy article titled “An Overview (and Criticism) of Methods to Detect Fake Content Online,” authored by Prof. Antonio Badia from University of Louisville, USA, discusses the issue of fake content online and proposes both human and algorithmic methods to solve the issue. One of the closing articles, “Hybrid Artificial Intelligent Multi-Layer Blockchain and Bitcoin Cryptology (AI-MLBBC),” authored by Prof. Murad Al Shibli from Abu Dhabi Polytechnic, UAE, provides new information on blockchain and bitcoin cryptology and explains new solutions that can be used to prevent hacking. The final article within this section, “ARM Hypervisor and Trustzone Alternatives,” authored by Prof. Nezer Jacob Zaidenberg from College of Management, Israel and Profs. Raz Ben Yehuda and Roee Leon from University of Jyväskylä, Finland, discusses the hypervisor vs. TrustZone™ implementation dilemma and explores new solutions.

Criminal activity and the world wide web are no longer a peripheral research topic. Instead, this is a very fast-growing research area which requires a tremendous amount of participation and collaboration by researchers from all over the world. The *Encyclopedia of Criminal Activities and the Deep Web* will aid in efforts to better understand and deal with the ever-growing societal problems and challenges that such devious activities present to individuals and organizations all over the world.

The diverse and comprehensive coverage offered within these articles will contribute to a better understanding of all topics, research, discoveries, and solutions in this evolving field. This publication will inspire its readers to further contribute to the current body of knowledge in this immense field, creating possibilities for further research and discovery into the future understanding of the dark side of the world wide web and how this technology has been overlooked in the past as an element of crime all over the world.

Mehdi Khosrow-Pour, D.B.A.

Editor-in-Chief

Encyclopedia of Criminal Activities and the Deep Web

Acknowledgment

Editing and completing an authoritative and comprehensive scholarly research publication such as the *Encyclopedia of Criminal Activities and the Deep Web* requires tremendous contributions, and a great deal of assistance from large groups of scholars and staff. The primary objective of this encyclopedia is to provide the most up-to-date scholarly coverage of all topics related to the evolving nature of criminal activity, especially online.

The contributed chapters from experts all over the world provide an in-depth look into topics such as cyber stalking, cyberterrorism, dating websites and crime, drug trafficking, e-banking fraud, gaming and crime, human trafficking, identity theft, online blackmail, online hate crimes, online predators, social media deception, vigilante justice, internet privacy information, cybersecurity legislation, child exploitation, internet regulations, international regulations on the dark web, and much more. I am indebted to all the authors for their excellent contributions to this publication.

All submitted manuscripts to this publication underwent a double-blind peer review process in order to achieve the highest level of quality and accuracy. I am thankful to all the reviewers of this encyclopedia for providing their expertise and their rigorous, unbiased assessment of the manuscripts assigned to them on a double-blind basis, as well as the members of the Editorial Advisory Board for their wisdom, guidance, and assistance with various decisions throughout the editorial process.

I would also like to convey my deep appreciation and gratitude to all those individuals who assisted me in editing this publication, which include Lindsay Wertman, Managing Director of IGI Global, Melissa Wagner, Managing Editor of Acquisitions at IGI Global, Chris Shearer, Copy Editing Manager at IGI Global, and Michael Brehm, Managing Editor of Book and Journal Production at IGI Global. Additionally, I would like to thank the IGI Global Sales and Marketing Department, especially Nick Newcomer, Senior Director of Marketing and Sales and Caroline Campbell, Marketing Manager, for their endless support in promoting this invaluable reference source.

Thanks to everyone who has provided me immeasurable amounts of knowledge, wisdom, and support over the last 30 years.

Mehdi Khosrow-Pour, D.B.A.

Editor-in-Chief

Encyclopedia of Criminal Activities and the Deep Web

Section 1

Cybercrime Profiles, Understanding Cybercrime, and the Realities of the Dark Web

Cybercrime

1

Poongodi Thangamuthu*Galgotias University, India***Anu Rathee***Maharaja Agrasen Institute of Technology, India***Suresh Palanimuthu***Galgotias University, India***Balamurugan Balusamy***Galgotias University, India*

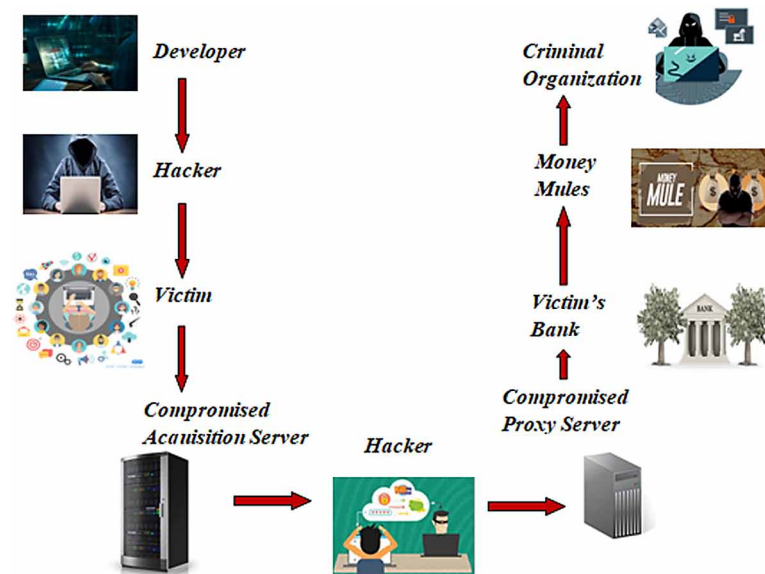
INTRODUCTION

The cybercrime prediction over the past year says about the damage cost by tracking the activities in government officials, industry experts, cybersecurity companies, universities, colleges, media outlets globally. A criminal way of doing an activity through the use of digital devices and internet by a group of people is known as cyber crime. The critical issue of cyber crime is pulling everyone's attention across the world. Due to the fast growth in e-commerce, e-governance, social networking and various other e-services cybersecurity has a growing challenge where database is easily collected and misused. Cyber attacks are more pervasive and threats to critical infrastructure and lack of security and underreporting makes industrial systems and products more vulnerable. Internationally, the most affecting problems are mass-ransomware attacks and valuable data theft much more in the last few years. Lack of electronic evidence in cybercrime and proper convergence between private, and government institutions are making difficult to seize and stop criminal financial transactions. Based on historical cybercrime statistics, there would be a dramatic increase in crime gang hacking activities and the cyber attack surface will be an order of magnitude greater in 2021 than today. According to the prediction of cybersecurity ventures, the cybercrime will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015. The estimated cyber security cost is rapidly growing to \$170 billion dollars in 2020 that was only \$75 billion Dollars in 2015. The European countries, making the directives used to protect the information in systems from threats, the first directive is EGDPR (European General Data Protection Regulations) and the second directive is NIS (Network Information Security).

The criminal activity of cybercrime includes the theft of intellectual property, damage and destruction of data, theft of personal data, stolen money, forensic investigation and reputational harm. Cybercrime is an online threat that can be committed by targeting the computer devices, computer networks and the automated processes performed through the use IT systems by creating and distributing malwares or viruses. Cybercrime allows attackers to penetrate in a well-controlled environment and the malicious activities remains untraceable. As it is a rapid growing area of crime, criminals exploit the convenience, speed, anonymity of the internet and committing various criminal activities by posing different threats

DOI: 10.4018/978-1-5225-9715-5.ch001

Figure 1. Cybercrime process



to victims worldwide on an unprecedented scale. The cyber crime process is explained in the following: Initially, the developer writes the malware code. Hacker uses the malware to exploit the credentials of victim's personal computer. For instance, bank account credentials are revealed to hackers from the victim's computer system and the hacker acquires the credentials of the target by compromising the server. The attacker gains the remote access to an individual's financial account in the victim's system and it is being stolen by manipulating the account from the concerned targeted bank by compromising the proxy server. The stolen fund is transferred to the money mule bank account and then it is transferred to criminal organization. The process of cybercrime is depicted in Figure 1.

Cyber attackers have the objectives for which they do cybercrime / cyber-attack (Kumar et al, 2014; Rawat et la, 2015). Significant objectives of cyber attackers are discussed below:

Entertainment

Some cyber attackers are performing criminal activities to examine their hacking abilities. Such persons are interested in getting fame in the cybercrime world. They feel proud of their successful attempts that were not achieved by any other attacker or some attackers failed to execute such kind of attack.

Hacktivists

These kinds of cybercriminals are stimulated by religious, social and political ends. Their intention is to inculcate the religious and political mottos among people and to depress them. It is an attempt of extending the religious or political popularity among the crowd. Recently, hacktivists are revealing the individuals secret affairs via social web sites.

Financial Gain

Attackers in this category desire to grow rich by performing criminal activities and focusing the financial gain. The targeted domain may be the large organization, banking systems, rich persons, or wealthy countries. Such type of attackers may be hired by some companies, individuals or countries for performing attacks.

Spying

In this category, the cybercriminals try to steal the confidential information of any specific individual, organization, or country. The spy hackers will work for their client's need and avail the payment in return.

Revenge

These kinds of cybercriminals may be formed because of irritated, humiliated and expelled employees. These persons knew the secret, weak points and policies of their organization, or country. The hackers perform their cyber-attacks by focusing the emotion of hate to take the revenge in the form of spoiling the reputation, financial loss, tarnishing the social image and so on.

Everyone in cybercrime is performing some task to fulfill their objective i.e., to gain the advantages in the perspective of money, revenge or any other motive. Various roles of criminal organizational members in cybercrime are shown in Figure 2.

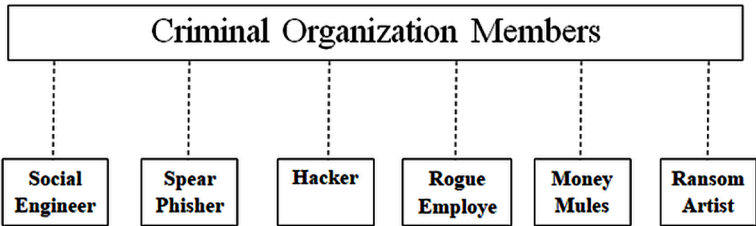
Different Perspectives of Cyber Crime

Cyber crime is broadly viewed as three categories based on the techniques and difficulty level (Haughn et al, 2017; Arlitsch et al, 2014).

Crimes Against People

In this category, a person disseminates illegal or fake information online which includes cyber stalking, harassment, child pornography, human trafficking, credit card fraud, identity theft and spoofing.

Figure 2. Criminal organization members in cyber crime



Crimes Against Property

Cyber criminal illegally gain access to get the confidential information such as individuals credit card details, make online purchase, and to execute phishing scams. It generally includes hacking, DDoS attacks, computer vandalism, copy infringement, cyber and type squatting.

Crimes Against Government

This type of crime is committed against government by hacking military websites, government websites, or distributing propaganda. It is an attack on nation's sovereignty and performed by terrorists or enemies of other nation. The cybercrime activities against the government comprise accessing confidential information, cyber terrorism, cyber warfare, and pirated software.

Taxonomy of Cybercrime

Cybercrimes are described as global crimes because they go beyond the geographical boundaries and can be perpetuated from anywhere against any individual or technology. The most occurring crimes in today's world are cybercrimes. Hackers are searching for new attack patterns that increase the complexity for security professionals to defend the data and resources on the internet (Singh et al, 2016). Hackers are affording free attack tools to increase the number of attack rate in the internet. The massive increase in e-services like online banking, online shopping and social apps gives a huge rise in the number of internet users which paves a way for easy target by cybercriminals (Wall, 2002). Some of the cyber crime activities happening in today's world are described below:

CYBER PEDDLER

Stealing confidential data from the computer system connected to the internet. There are two types of cybercrime in this activity,

Cyber Fraud

It is a fraudulent activity of making personal or financial gain by deception. It encompasses social engineering attacks like spear phishing, password guessing and DNS redirecting in which the attacker will acquire and use the confidential information of various users.

Cyber Activism

Social applications are used to create, operate, manage the activism and the information will be distributed to large number of users in few seconds. The communication technologies used are WhatsApp, Twitter, YouTube, Facebook, Gmail, LinkedIn, etc. Moreover, these technologies have been made for affording better connectivity with colleagues, friends and the latest information can be reached quickly to a wide geographical area. But the person with wrong intention uses these technologies for spreading rumour to spoil the image or sending false information about individuals or organization to avail some benefits.

CYBER VIOLENCE

1

It means the violence is created using any device (like smartphone) or computer system connected to the internet. The impact of “violence” will be harmful and the components that are affected may be the data on servers, devices connected to the internet, and any individual or entire organization can be devastated by cyberviolence. The different forms of cyberviolence are discussed,

Cyber World War

The violence created at maximum level that affects many countries in the world. The cyberworld war may act upon an individual, whole country, military sector, private as well as government employees. The main goal of this attempt is malfunctioning or to disable, destroy the infrastructure of any adversary and to attain the victory of the targeted country.

Cyber Terrorism

Some set of people has only the aim of destroying the peace of humanity known as terrorists. They believe that the thing they are doing is right to enrich their religion stronger in the world or they have the privilege to command over the world or no other can be powerful than them. These kind of malicious activities in the digital world are referred to as cyberterrorism. The people who are involved in these activities will not have any sympathy or emotions. They will behave like machines for using any type of attack to fulfill their objective.

Cyber Stalking

It is a crime in which the attacker annoys a victim through the electronic communication by sending e-mail or instant messages (Sreenivasulu et al, 2013). A cyberstalker utilizes the anonymity in the internet to stalk the target without being detected. The most precautionary way is to use primary e-mail account only communicating with the trusted persons and maintain anonymous mail account for all other communications. Moreover, it is suggested that not to place any personal details in an online profile.

Cyber Revenge

It is a criminal activity which is harmful against someone in reaction to one's previous action. The main objective is to destroy the adversary by revealing the confidential information, forming the false image in the internet system, and destroying computer based resources. Revenge hacking encompasses the extensive set of drive behind cybercrime. The victimized industries have to face various forms of cyber-attack that links back the own hostile policies or actions towards the attackers. A target server is considered as the source of a threat and in particular, it may be the component of a hospital, public utility or any municipal authority. Attackers comprise a server as a proxy one for launching attacks across the global. Moreover, there is a constant probing in automated systems that can easily allow cracked access credentials.

CYBER SQUATTING

In this type of cybercrime, the attacker registers the name of the trademark of others illegally as their domain name such that the owner fails to register the domain name with their own trademark. The different types of cybersquatting are as follows:

Classic Cyber Squatting

The main goal of the cybersquatter is to obtain ransom from the target. Once the cybersquatter gets paid from them, then the attacker deletes or sells off the domain name. Nowadays, due to enforcement of laws this type of attack is not more popular.

Derogatory Cyber Squatting

In this category, the attacker tries to destroy the reputation of the target. The illegitimate activities are done by uploading violated contents, hate speech or any pornographic material on the domain name.

Typographical Cyber Squatting

In this type of attack, the hacker cannot use the same name of the trademark because the domain name is already being registered by the owner of the trademark. Hence, the hacker uses the domain name very similar to the original one. For instance, if the hacker is using the registered domain name such as Yahoo mail which is very similar to Yahoo mail, then the adversary may succeed to make some losses for the original trademark owner.

CYBER TRESPASS

Trespass refers to the illegitimate activities that someone crosses boundaries for accessing the information without any authorization. It is the crime where cyber law is violated by accessing an authorized user system. It also violates the fundamental security services such as integrity and confidentiality. The various types of cyber trespass are discussed below:

Cyber Theft

Theft is a threatening activity that something is stolen or damaged. In real world, damaging or stealing something physically into someone's property like in organization or houses and stealing some valuable things such as file, gold, and so on. Cyber theft in cyber world is occurred by technically hacking computer system connected to the internet. The main objective of hackers in cybercrime is to steal data in the cyberspace for personal or financial gain. Basically, the theft in cyber crime can be done in two ways:

Theft to Data/Information

Some confidential information of organization, individual and country can be hacked. Various security services like confidentiality, integrity and availability of information must be managed carefully from cyber attackers.

Theft to Cyberspace

Cyberspace is not able to manage in a controlled manner then it leads to malfunction. Hackers have the objective of stopping the target services or attack them directly in the cyberspace.

Cyber Espionage

It refers to cyber spying and it is an act of monitoring the activity of individual, organization, company, country, rival or enemy by carrying out the malicious activities in the network. These activities are performed by technically strong persons which are difficult to trace. Attackers start analyzing the network traffic illegally, uses laptop cameras and security cameras to acquire the information about targets, i.e., some personal information like what kind of work they are doing, type of information they are accessing etc.

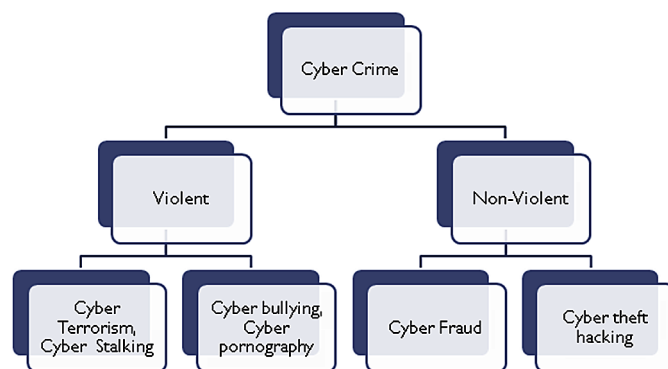
a) Cyber pornography

Cyber pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber pornography is a criminal offense, classified as causing harm to persons. In this type of attack, the attacker uploads sexual material of a person on public websites. One of the biggest publicized catches of child pornography perpetrators was launched in May 2002 and called Operation Ore. The intruder will hack the private pictures of a person by targeting their mobile, tablet, security cameras or computer system. Exposing private pictures or videos makes embarrassed to the target of an adversary. In some extreme cases, the person commits suicide attempt also.

GENERAL DESCRIPTION OF CYBER ATTACK

The monitoring, regulation, protection, and enforcement related to cybercrimes are not solely responsibilities of state-controlled public police. This stresses the need for alternative strategies to cope with the policing deficit. A possible strategy to overcome such problems is an integral approach, which is an approach wherein all relevant stakeholders—public as well as private—participate in the implementation of safety and security policy. An outgrowth of such an integral approach is a Public–Private Partnership (PPP). To provide this safety to the people cyber attacks are basically categorized into violent and non-violent as depicted in Figure 3. The violent category of cyber attacks includes cyber terrorism, stalking, bullying, pornography. Non-violent cyber crime comprises of fraud, cyber theft hacking. Cyber Bullying is most common over past five years; In this, generally the people below eighteen ages are more susceptible as per the study. Cyber Bullying is a threat when a person receives negative comments or pictures from the person on another side.

Figure 3. General category of cyber attack



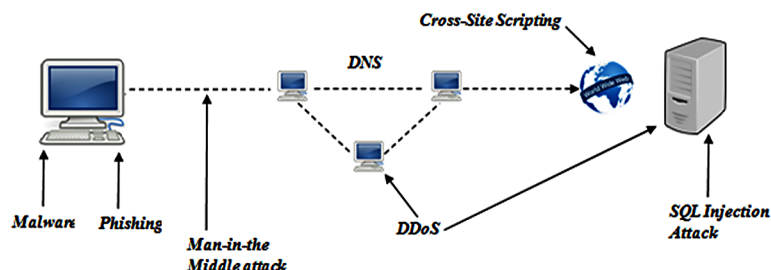
A variety of cyber-attacks are tremendously increasing day by day in the world of internet and it continues to evolve. Attackers gain access to the system, locking sensitive files, leaking proprietary information to the public, and stealing mission-critical information. Moreover, it is very hard to recover from such types of attacks in large scale enterprises (Zulkefli et al, 2015). Many cyber-attacks are immensely destructive which follow diverse strategies to capture different ends. Ransomware is the malicious software designed to damage or controls the computer system. Phishing introduces fake official emails, fake websites where victims log in and enter their passwords. In Man-in-the-Middle attack, hackers insert themselves between the computer and the web server. Distributed Denial of Service overloads the server with bogus data leads to unavailability of service. Cross-Site Scripting injects the malicious code into a website which target's the victim's browser. SQL injection attack corrupts data to make a server disclose the sensitive information such as credit card number, username etc. The block diagram of cyber-attack is given in Figure 4.

Some of the most significant cyber-attacks are explained in the following sections.

Ransomware

Ransom malware or ransomware is the digital version of kidnapping, which prevents the normal users for accessing the personal files from their system and demands for random payment to regain the access. The first version of ransomware was originated in late 1980s and the payment was to be paid through snail mail. Nowadays, the ordered payment is to be sent via credit card or cryptocurrency. Typically, hacker

Figure 4. Block diagram of cyber attack



places the ransomware file in the targeted server and follows some form of phishing for transmitting the malicious file along with email of an intended user. Once the user opens the file, the malicious ransomware file is deployed in the user's system and encrypt, locks the highly sensitive files. If the user tries to open the file, they are intimidated with the message as "files have been locked". It is possible to receive the encryption key once the user paid the specified amount to the hacker, usually done through bitcoin payment which is untraceable. However, over 85% of the malware targeting medical devices in 2018 was ransomware. Ransomware attacks of 2017, namely, Cerber and Jaff. Cerber is a family of ransomware payloads which are distributed through exploiting kits, email, JavaScript, and Microsoft Word macros. Variants of Cerber include a Bit-coin wallet stealing function. Jaff is described as new but vicious. It is spread via the Necurs botnet and is downloaded in a .pdf file attachment. Jaff is said to check for the target computer's language setting. This attack is massively growing in the recent years and some of the ransomware are mobile ransomware, leakware, doxware, encrypting or non-encrypting ransomware.

Internet of Things

Internet of Things is made up of digitally connected devices to the internet which makes people lives easier (Sadeghit et al, 2015; Weber et al, 2016). IoT sector is anticipated to grow up to 20.4 billion devices by 2020, and the business sector is expected to spend \$134 billion by 2022 only for cyber security on IoT devices. The IoT devices are more vulnerable to various types of attacks. The associated gadgets or machines are a great degree profitable to digital attacker for few reasons. Most IoT gadgets work unattended by people is very simple for an attacker to physically access them. Most IoT parts impart over remote systems where an attacker could acquire private data by listening in. Many IoT devices are puzzled with security holes, where hackers can pass through easily to accomplish malicious activities. It leads to catastrophe on a large scale and in 2016, IoT attack was launched that ends in huge portions of the internet become inaccessible. In workplace, the average number of IoT devices is anticipated to increase from 9,000 to 24,762 devices. This issue presents a significant threat to all organizations, because more IoT devices are interconnected to the network.

Social Engineering and Phishing

In social engineering attack, attacker prefers the human interaction to compromise the computer systems or an organization (Yar et al, 2013). An attacker pretends to be a researcher, newly joined employee, offering credentials to support the identity. Spear-Phishing refers to identify and prevent the targeted email attacks which are entering the organization (Sood et al, 2013). Attackers in phishing attack broadcast a large net in the anticipation of catching anyone, whereas spear-phishing attackers highly focusing the targeted victim. The most common targeted victim in spear-phishing attack is the high ranking employees and it is very hard to protect all users from the attackers.

Some of the challenges in Spear-Phishing: It is an on-going illegitimate activity in the cybercriminal, hacktivist and nation-wide attackers' cache. It is an inexpensive and effective method to implant different forms of malware, collect user credentials, bring unexpected users to malicious websites, mimic trusted persons and organizations, and harvest valuable information about the targeted organization. Many users are deceived by spear-phishing emails (Moon et al, 2015) on believing the attackers consistently.

Man in the Middle Attack

In this type of attack, two original parties involve in communication normally in an unsecured wireless network. The sender does not know the receiver is an attacker trying to modify the message before retransmitting to the original receiver. Hence, the attacker has a control over the communication. For instance, Wi-Fi in the organization is unsecured; an attacker may intercept any information being transmitted from the employee's system. It can be prevented by installing Virtual Private Network [VPN] in employee's system, still there is a risk if the information is being captured from personal devices such as mobile phones and tablets.

CYBER ATTACKS BASED ON SECURITY PRINCIPLES

Cyber attacks are the activities executed by the cybercriminals to break the fundamental principles of cybersecurity (Liu et al, 2012) in the internet world. Cyber attack is a special form of cybercrime that accomplishes crimes/attacks in cybersecurity. The different forms of cyber attacks based on the cybersecurity basic principles are discussed below:

Attacks on Confidentiality

The various types of attacks based on confidentiality are as follows:

Traffic Analysis

In this type of attack, the attacker tries to analyze the information which is transmitted between the sender and the receiver without tampering it. It is a kind of passive attack and the attacker analyses the information to interpret some new information by stealing the confidential data. It results in violating the confidentiality principle of information security.

Eavesdropping

It refers to the activity of listening the confidential conversation secretly. The intruder track and capture the information which is transmitted between the sender and the receiver. It is similar to traffic analysis, whereas the intruder can sniff the information that can be read later according to their interest.

Snooping

It is a kind of passive attack, where the intruder tries to find the confidential information about users by hacking the personal details such as online banking, social apps, login credentials of email etc. The government officials or the corporate sector exploit the snooping methodology for monitoring the employees' activities. Snooping is categorized into two types as given below:

1. **Digital Snooping:** It is the process of tracking the private or public network to know some confidential information such as data or password. This type of attack is done at the network layer via the physical cable. The attacker may alter the network devices such as switches to acquire the

information passing in the network. To avail the organization data as authorized users, the attackers can hack the organization security cameras to obtain the username and password of employees.

2. **Shoulder Snooping:** It is a kind of physical attack where someone watches the typed password or information displaying in the monitor for that they don't have any access.

PASSWORD ATTACKS

These types of attacks are used to obtain the username and password of desktop, laptop, website or any other applications of authorized users. The retrieved username and passwords are used to get enter to network services as authorized users and to perform malicious activities. The success of this password attack depends on users password strength. If the chosen password is not weak, it is difficult for the hacker to get access to the authorized user's password. The types of password attacks are discussed below:

Dictionary-Based Attack

The attacker tries the possible combination of characters or words as given in the dictionary to hack the password of internet applications of legitimate users. The success of this attack depends on the strength of authorized user's password. If the chosen password is not available in the dictionary, then this type of attack is almost impossible to be performed by the attacker for hacking the password of the user.

Brute-Force Attack

It is a tool to hack the user password by trying all possible password combination. It is a time consuming activity based on the strength of password. However, it results in obtaining the authorized user's password.

Password-Guessing Attack

In this attack, attackers guess the password of legitimate users by using some common words such as name, date of birth, religion and so on.

Keylogger

It is a kind of malware that executes in the hidden mode on the system background, the user is unaware about the execution of keylogger. It may be in the form of icon, quick launch, entry on desktop, all programs and so on in the computer system. The information typed by the user is scanned by the keylogger and that will be transferred to the attacker without user's knowledge (Solairai et al, 2016).

Social Engineering

It is kind of attack that focuses small set of internet users and revealing information of authorized users of an individual or an organization (Krombholz et al, 2015). The types of social engineering attacks are given below:

Phishing

In this attack, the attacker tries to trick the users for hacking sensitive information such as credit card details, bank user id/password. Fake websites, emails are used by the attacker whereas it looks same as the original and it covers small to large set of network users (Mohammad et al, 2014). The various categories of phishing attacks are described below:

DNS Phishing

It is a process in which the attacker modifies the host files on victim's system or DNS database hence the legitimate web URL is modified as a fake URL. By assuming the fake website as original, the users start to feed the confidential information in an unauthorized site. Sometimes, technically strong persons also fail to differentiate the authorized and fake website (Chaudhry et al, 2016).

Spear Phishing

In this type of attack, the attacker searches for the available public information of the target via social networking or web sites. Subsequently, an attacker creates malware exist email to earn the victim's trust. Then this mail is forwarded to some set of targeted people and if anyone clicks on it, they will become as the victim. An attacker will hack the confidential information because the malware attached email works automatically when an email is opened.

Dumpster Diving

Attacker seeks confidential information of an organization or the network user without any use. For instance, the attacker searches the trash of an organization to get some sensitive information (Lau et al, 2015).

Baiting Attack

In this attack, the attacker sets the malware infected storage device at the place where the victim may notice in future. The storage devices are labeled in such a way of increasing the curiosity of target and once the storage media is accessed, the computer system will become as a victim of the attacker (Krombholz et al, 2015).

Waterholing

In this attack, an attacker indirectly targets the victim by infecting the websites where the target frequently visits. Hence the target's computer device will get affected and the attacker starts stealing the confidential details (Krombholz et al, 2015).

Reverse Social Engineering

The attackers represent themselves as trusted persons to the victim and they believe that the attacker is a trustworthy person to share the confidential details.

ATTACKS ON INTEGRITY

The different types of attacks to disrupt the integrity as follows:

Salami Attacks

Set of minor attacks that altogether result in the form of larger attack. For instance, deduction of less amount of money from the bank account is not noticeable. Once it becomes huge, it spoils the image of the bank.

Data Diddling Attacks

It is an activity of illegal data modification. For instance, account executives alter the timesheet information of employees before reaching the payroll application.

Cross-Site Scripting (XSS)

Attacker inserts malicious script into vulnerable websites or applications that the target visits. The hacker's malicious code is automatically transferred to victim's browser, once the target visits the vulnerable website. The malicious code accesses the sensitive information from the victim's browser (Kieyzun et al, 2009).

SQL Injection Attack

It is similar to cross-site scripting rather it uses the vulnerabilities of SQL statement. It affects the websites, web application database and the information in the database is revealed to the attacker (Kieyzun et al, 2009).

Session Hijacking Attacks

Attacker modifies the session among two or more authorized users to gain the authorized access of information. Example: Man-in the middle attack, TCP Session hijacking.

Attacks on Availability

It refers the process to disrupt or stop the availability of required resources to the authorized users. The few common attacks are described below:

DoS/DDoS

Denial of Service (DoS) is an attack that interrupts the availability of network resources. The victim can be targeted either directly or indirectly. In direct attack, the hacker creates huge traffic by using the own computer system, while in indirect attack, the hacker hacks another system refers as "bots" to create the traffic for the victim. In DDoS, huge number of bots or a server can be used to disrupt the network services such as system resources, application resources, and network bandwidth (Zlomislic et al, 2014; Osanaiye et al, 2016). The various consequences of DoS attack,

- Slow network performance
- Unavailability of network services

The different types of Dos/DDoS attacks are discussed below:

TCP SYN Attack

In this attack, attacker utilizes the loop-hole of the three-way handshake process during the connection establishment of TCP (Transmission Control Protocol).

Steps in three way handshake protocol:

1. Client sends SYN (Synchronization) request to the server
2. Server gives response with ACK (Acknowledgement) to the client
3. Clients, in turn respond with final ACK

Attacker broadcasts SYN requests and never transmits the final ACK which leads to overflow of the target capacity results in unavailability of network resources (Pan et al, 2006).

UDP Attack

TCP and UDP [User Datagram Protocol] are the transport layer protocol in TCP/IP model. TCP is reliable, connection-oriented protocol and UDP is unreliable, connection-less protocol. In connectionless, reliability can be compromised to some extent and the attacker generates huge amount of UDP packets to overflow the response handling queue which leads to unavailability of network resources to the users (Pan et al, 2006).

ICMP Attack

ICMP (Internet Control Message Protocol) is a network layer protocol used by network devices such as routers to generate the error report if any problem is encountered during delivery of IP packets. Attacker generates the huge traffic of ICMP traffic to the targeted host which automatically consumes the bandwidth.

ICMP attack can be done in two ways:

1. Ping of death attack
2. Smurf attack

Ping of Death Attack

It is a mechanism to check the availability of particular IP packets using small packets. Attacker sends large-size packets than the maximum packet size. The target may crash or reboot though it is not configured with the large-size packets.

Smurf Attack

1

It follows the amplification strategy and it targets the Internet Broadcast Address (IBA) which is in IP protocol. Attacker sends request by spoofing the address of the target to IBA of the intermediary node reply with amplified response to the target node. The intermediary response is broadcasted to all hosts and IBA can support upto 255 hosts. Hence, the smurf attack amplifies a ping 255 times (Barnett et al, 2000).

HTTP Attack

HTTP (Hypertext Transfer Protocol) is an application layer protocol of TCP/IP model. The web applications and services use HTTP packets such as GET and POST request. Hackers transmit huge amount of GET or POST request to the target host results in overwhelming the target capacity (Barnett et al, 2000).

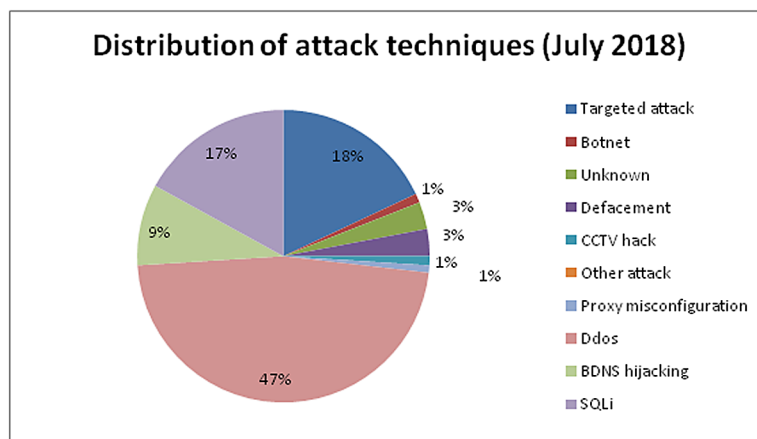
CYBERCRIME STATISTICS

Most of the cyber-attacks are focused against only small scale businesses. According to Cybersecurity Ventures Prediction, victim to a ransomware attack increases from every 40 seconds in 2017 to every 24 seconds by 2019. In the past 2 years, it has been recorded that the ransomware damages up to 15X and it is expected to quadruple by 2020 in healthcare organizations. FBI's BEC (Business Email Compromise), Internet Crime Complaint Center (IC3) the total amount of loss has been increased 1,300 percent since January 2015 at more than \$3 billion. According to the CISCO's, BEC has viewed the identified exposed losses totaling over \$5 billion from 2013 through 2016, and the losses persist to mount. According to the global survey conducted previous year by the Microsoft Digital Crimes Unit, 2 out of 3 people have experienced the technical support scam in the last 12 months. The cyber criminals are generating around 1.4 million phishing websites with fake pages to impersonate the targeted company which they're spoofing. The distributed denial-of-service attacks are 4X larger than the status before two years – it is about 42% of DDoS incidents in 2017, from 10% of cases in 2015. Cybersecurity Ventures anticipates that recently reported zero-day exploits will mount from one-per-week in the year 2015 to one-per-day by 2021. According to the study report of 2018, the distribution of attack techniques are depicted as shown in the Figure 5.

IMPACT OF CYBERCRIME ON SOCIETY

Cybercrime has become a major threat for the persons using internet, millions of information are being stolen within the past few years (Jang-Jaccard et al, 2014). The global cost of cybercrime may reach \$6 trillion by 2021 in an economy era. According to the study of Data Breach Study of Ponemon Institute's 2016, Global Analysis organizations that experienced one breach in 2016 lost an average of \$4 million. 48% of data security breaches are caused due to malicious activities. Cybercrime will triple the number of unfilled cybersecurity job opportunities by 2021.

Figure 5. Distribution of attack techniques



Cyber Crime Security

Securing IT infrastructure and countermeasures for various attacks are mandatory as the cyber attacks are increasing every day due to technology advancement. Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft. Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access (Razzaq et al, 2013). Although finding out the countermeasures for these attacks are not easy and its quite complex because of a number of layers of defense. Developing a single suite for managing all these attacks is very difficult due to the existence of several layer of defense (Barnett et al, 2016). The ratio of threat is increasing as the probability of risk is also increasing day by day and organizations should consider the information security as the primary concern.

None of the small, medium or large organization around the world is completely safe since the cyber attacks happen every second. Nation-wide attackers and cyber attackers gives the biggest information security threat around the globe. According to the report of Center for Strategic and International Studies (CSIS), cybercrime expenses the global economy on \$445 billion and the harm to businesses from attackers stealing intellectual property exceeds \$160 billion every year. Based on the study over 15 million attacks gathered throughout various news and events, FBI (Federal Bureau of Investigations), CISCO, Cenxic, FireEye, Kaspersky, Verizon, Mandiant, Sophos and Syumantec, the cyber-attack is an on-going trend, strengthened by hacker's efficient tools and strategies by hiding their presence for obtaining sensitive information.

According to the report, "Attacks on IoT devices increases rapidly because of weak security hygiene, exponential growth in the amount of connected objects, and the huge volume of data in IoT devices" and it is anticipated that by 2019, the devices connected to the internet will be 50 billion. The new strategies are continuously developed by the attackers to exploit the data and network. Some study reveals that the root-cause of security breaches in 50% of criminal intended attacks are based on three significant factors: system vulnerabilities, human error and intended attack (Liu et al, 2012). Basically, there are two categories of cyber crime security measures that are viewed as external and internal.

External

Many nonprofit organizations are combating against cyberattacks, International Association of Cyber-crime Prevention (IACP) or Secure Domain Foundation (SDF) are assisting to be aware of attacks, risks and states how to defend against attacks. Moreover, Google recently forms a team known as Project Zero to mitigate the cyber-attack risk and to analyze the bugs, vulnerabilities by taking the necessary steps for improving the software products. Cyber-attacks also entered in financial institutions, AXA Corporate Solutions is a financial company launched an insurance product covers the expenses to recover after some errors or accidental events, viruses and cyber attacks. Additionally, another product is also launched for assessing and mitigating cyber risks. The legal approach is the most essential aspect regarding cyber crime and security. Although the laws and regulations are constantly developed to limit or prevent the cyber-crime activities, however these set of laws and regulations are geographically limited to certain level.

Internal

Continuous Risk Assessment

Every organization should implement the security controls and the necessary steps should be taken to identify threats, vulnerability and risks. IT based companies should ensure that all hardware, software including protection software (i.e. antivirus program) is always updated with the latest patches. Moreover, the agreement is mandatory for companies in place of third party to cover the maintenance and upgraded services.

Authentication

Focusing on the risk assessment, the organizational data is solely protected using the password technique. For remote or web-based applications, complex authentication strategies are recommended to use. For instance, combining password and biometric authentication is a complex authentication mechanism.

Internal Commitment and Responsibility

Risks are more often in the organization premises than expected, some security breaches can be caused even unintentionally by the internal users. Hence, formalize the set of policies, procedures in a concise manner by well documenting the controls and processes assist in maintaining and enriching the information security.

Access to Information

Organizations should always ensure that the privilege is properly restricted and the session for outsiders should be correctly disabled who has connection to the company's network. A wide range of risks, addresses various issues from manual to automated controls. Manual control can be accomplished by conducting the periodic review of access rights for all users and with the automated control, the domain account is automatically terminated once if it is not connected for a certain amount of time.

Data Retention

Removing all data if no longer required, in such a way compromising information security policies can be avoided. The data archive should be maintained as long as it is required on a secured environment (back-up servers) and eradicated from the organization's network, therefore limits the unauthorized access to sensitive data. The study revealed that 20% of stolen information was the data without any evidence in the company's network.

Threat Intelligence

There are numerous ways to collect threat intelligence. For instance, the intelligence can be purchased directly from security vendors in a report format. And there is a possibility to join in an intelligence sharing group such as financial service industry's (FS-ISAC) to know about the threat. Intelligence can also be retrieved by own by examining the incoming connections in the network. Intelligent gathering process is an on-going process in many organizations to widen the threat intelligence capability. Hence, combining intelligence into a single source plays a vital role in security related operations.

Minimize Delivery of Malware

Social engineering is the most common strategy to reduce the malware or threat introducing vulnerabilities. There are numerous ways to allow the threat in an organization, such as phishing or leaving USB in the company premises and unintentionally it may lead to some harmful action.

Organizing information security related programmes very often in an organization assist in creating awareness about security breaches. Advance technical controls are existing nowadays; even though human resource is considered to be the main source in spreading malware. By using registered software's on all computers, the chances for the threat of cyber attack can be extensively reduced. Corrupted or Pirated versions are the main reasons for introducing malware in the network.

GUIDELINES TO DEFEND CYBERCRIME

In the modern age of technology, no one is safe and secure in the internet world. The average dwell time is considered to be more than 200 days for a company to detect the cyber breach. Moreover, the internet users do not believe in the fact that they may get attacked of not updating the passwords or other credentials frequently. It gives the opportunities for hackers to perform cyber crime activities. The ways to prevent execution of malware are least access privileges, application white listing, Identity and access management, Network restrictions/segmenting to be strictly followed. The life cycle of preventing cyber crime is illustrated in Figure 6.

Identify the hackers immediately once they enter in IT infrastructure. Protect the environment by maintaining updated versions and detect the malicious activity done by the attacker (Ali et al, 2015). Provide the fast response and recover from the scenario to continue the process without any disruption.

Figure 6. Steps to prevent cyber crime



Authorized users should be aware on the preventive measures to protect the individual as well as the business sector. Some significant strategies to be followed for preventing cyber crime,

1. Be vigilant when surfing websites
2. Choose VPN whenever possible
3. Make sure the websites are safe before entering credentials
4. Maintain antivirus or application systems up to date
5. Strengthen the password, never use weak password
6. Flag and report suspicious emails
7. Never click the unfamiliar links

CONCLUSION

The world is facing a massive problem in ensuring the proper security of information. To handle the problem due to the exponential growth of cyber crime is a world-wide awareness, from an individual to organizational perspective in the cyber world. Probably, the legal aspect is the main barrier in every state or region which has their own set of laws and regulations governing the attack of data privacy and theft. Internet is acting as the most powerful tool for the attackers in cybercrime. The only possible way to defeat the cybercrime is to think and act globally regarding the safety and rights of citizens in the whole world.

REFERENCES

- Ali, S. T., Sivaraman, V., Radford, A., & Jha, S. (2015). A survey of securing networks using software defined networking. *IEEE Transactions on Reliability*, 64(3), 1086–1097. doi:10.1109/TR.2015.2421391
- Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, 54(1), 46–56. doi:10.1080/01930826.2014.893116
- Barnett, S. (2016). Top 10 challenges to securing a network. *Network Security*, 2000(1), 14–16. doi:10.1016/S1353-4858(00)86652-0
- Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, 10(1), 247–256. doi:10.14257/ijisia.2016.10.1.23
- Dewan, P., Kashyap, A., & Kumaraguru, P. (2014). Analyzing social and stylo metric features to identify spear phishing emails. *Electronic Crime Research (eCrime)*, 2014 APWG Symposium on, IEEE, 2014, 1–13.
- Haughn, M., & Gibilisco, S. (2017). *Confidentiality, Integrity, and Availability (CIA Triad)*. Retrieved from <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cyber security. *Journal of Computer and System Sciences*, 80(5), 973–993. doi:10.1016/j.jcss.2014.02.005
- Josang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2), 618–644. doi:10.1016/j.dss.2005.05.019
- Kang, J., & Lee, D. (2007). Advanced white list approach for preventing access to phishing sites. *Convergence Information Technology, 2007. International Conference 2007*, 491–496. 10.1109/ICCIT.2007.50
- Kaster, P., & Sen, P. K. (2014). Power grid cyber security: challenges and impacts. *Proceedings of the 2014 North American Power Symposium (NAPS)*, 1–6. 10.1109/NAPS.2014.6965424
- Kieyzun, A., Guo, P. J., Jayaraman, K., & Ernst, M. D. (2009). Automatic creation of SQL injection and cross-sites cripting attacks. *Proceedings of the 31st International Conference on Software Engineering (ICSE 2009)*, 199–209. 10.1109/ICSE.2009.5070521
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. doi:10.1016/j.jisa.2014.09.005
- Kumar, G., Kaur, A., & Sethi, S. (2014). Computer network attacks a study. *International Journal of Computer Science and Mobile Applications*, 2(11), 24–32.
- Lau, L. B., Singh, M. M., & Samsudin, A. (2015). *Trusted system modules for tackling apt via spear-phishing attack in byod environment* (Thesis). Universiti Sains Malaysia.
- Liu, J., Xiao, Y., Li, S., Liang, W., & Philip Chen, C. L. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys and Tutorials*, 14(4), 981–997. doi:10.1109/SURV.2011.122111.00145
- Markey & Atlasis. (n.d.). *Using decision tree analysis for intrusion detection: a how-to guide*. SANS Institute.

- Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Intelligent rule-based phishing websites classification. *IET Information Security*, 8(3), 153–160. doi:10.1049/iet-ifs.2013.0202
- Mokhtar, B., & Azab, M. (2015). Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal*, 54(4), 1115–1126. doi:10.1016/j.aej.2015.07.011
- Moon, D., Im, H., Kim, I., & Park, J. H. (2015). Dtb-ids: An intrusion detection system based on decision tree using behaviour analysis for preventing apt attacks. *The Journal of Supercomputing*, 1–15. doi:10.1007/11227-015-1604-8
- Osanaiye, O., Raymond Choo, K.-K., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, 67, 147–165. doi:10.1016/j.jnca.2016.01.001
- Pan, Y., & Ding, X. (2006). Anomaly based web phishing page detection. *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, 381–392.
- Rawat, D. B., & Bajracharya, C. (2015). Cyber security for smart grid systems: status, challenges and perspectives. *Proceedings of the Southeast Con 2015*, 1–6. 10.1109/SECON.2015.7132891
- Razzaq, A., Hur, A., Farooq Ahmad, H., & Masood, M. (2013). Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. *Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, 1–6. 10.1109/ISADS.2013.6513420
- Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 201552nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 1–6. 10.1145/2744769.2747942
- Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security and Privacy*, 11(4), 3–4. doi:10.1109/MSP.2013.84
- Sheng, S., Wardman, B., Warner, G., Cranor, L. F., Hong, J., & Zhang, C. (2009). An empirical analysis of phishing blacklists. *Proceedings of Sixth Conference on Email and Anti-Spam (CEAS)*.
- Singh, S., Jeong, Y.-S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, 200–222. doi:10.1016/j.jnca.2016.09.002
- Solairaj, A. (2016). Keyloggers software detection techniques. *Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 1–6.
- Sood, A. K., & Enbody, R. J. (2013). Targeted cyber attacks: A superset of advanced persistent threats. *Security & Privacy, IEEE*, 11(1), 54–61.
- Sreenivasulu, N. S. (2013). *Law Relating to Intellectual Property*. Gurugram, India: Partridge Publishing.
- Wall, D. D. S. (2002). *Crime and the Internet*. London: Routledge.
- Weber, S. H., & Studer, E. (2016). Cybersecurity in the internet of things: Legal aspects. *Computer Law & Security Review*, 32(5), 715–728. doi:10.1016/j.clsr.2016.07.002
- White, J. S., Matthews, J. N., & Stacy, J. L. (2012). *A method for the automated detection phishing websites through both site characteristics and image analysis* (Vol. 8408). doi:10.1117/12.918956

Xenakis, C., & Ntantogian, C. (2014). An advanced persistent threat in 3g networks: Attacking the home network from roaming networks. *Computers & Security*, 40, 84–94. doi:10.1016/j.cose.2013.11.006

Yar, M. (2013). *Cybercrime and Society*. Thousand Oaks, CA: SAGE Publications.

Zhao, G., Xu, K., Xu, L., & Wu, B. (2015). Detecting apt malware infections based on malicious dns and trac analysis. *IEEE Access: Practical Innovations, Open Solutions*, 3, 1132–1142. doi:10.1109/ACCESS.2015.2458581

Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., . . . Yue, C. (2016). The highly insidious extreme phishing attacks. *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, 1–10. 10.1109/ICCCN.2016.7568582

Zlomislic, V., Fertalj, K., & Sruk, V. (2014). Denial of service attacks: an overview. *Proceedings of the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9), 1727–1765. doi:10.1109/JPROC.2016.2558521

Zulkefli, Z., Mahinderjit-Singh, M., & Malim, N. (2015). Advanced Persistent Threat Mitigation Using Multi Level Security Access Control Framework. *Lecture Notes in Computer Science*, 9158, 90–105. doi:10.1007/978-3-319-21410-8_7

A Survey on Emerging Cyber Crimes and Their Impact Worldwide

1

Suraj Gangwar*University of Delhi, India***Vinayak Narang***University of Delhi, India*

INTRODUCTION

Cybercrime is an unlawful act wherein the computer is a tool or target or both. The number of cybercrimes has escalated in recent times. The opportunity for cybercrime is increasing with the increasing number of internet users. In the year 2016, it was reported as the second most commonly reported crime across the world. Report published by World Economic Forum placed cybercrime in top five of the global risk for 2018 (The Global Risks Report 2018 (13th Edition), 2018). The reason behind is simple: the rate of internet connections and the ever growing number of computer devices are outpacing our ability to properly save them (Security Predictions for 2018 Paradigm Shifts, 2017). In today's increasingly connected digital world, organisations are too hyper-connected with a new wave of technologies to improve their performance. At the same time cyber-attacks are becoming more sophisticated and impactful (Cybersecurity Regained: Preparing to Face Cyber Attacks, 2017). Embracing of technical innovations such as the Internet of Things (IoT), cloud computing and AI/ML, by organisations provides cybercriminals with new avenues for attack.

As per a report generated by Global Cyber Security Index (GCI), it can be inferred that majority of the countries in world are not yet ready to deal with cyber-attacks. GCI categorizes the countries depending upon their level of cyber security. It divides the countries in three stages

1. Leading stage: which includes countries that show high commitment to face cyber-attacks
2. Developing stage: which includes countries that are increasingly digitized but are still developing their cyber security capabilities
3. Initiating stage: which includes countries whose economies are only beginning to be digitized and where cyber security efforts are just a beginning.

The 2017 report reveals that only 21 countries are at a leading stage and 96 countries are still at the initiating stage. So there is still much needed to be done to tackle cybercrime menace efficiently (Global Cybersecurity Index (GCI), 2017).

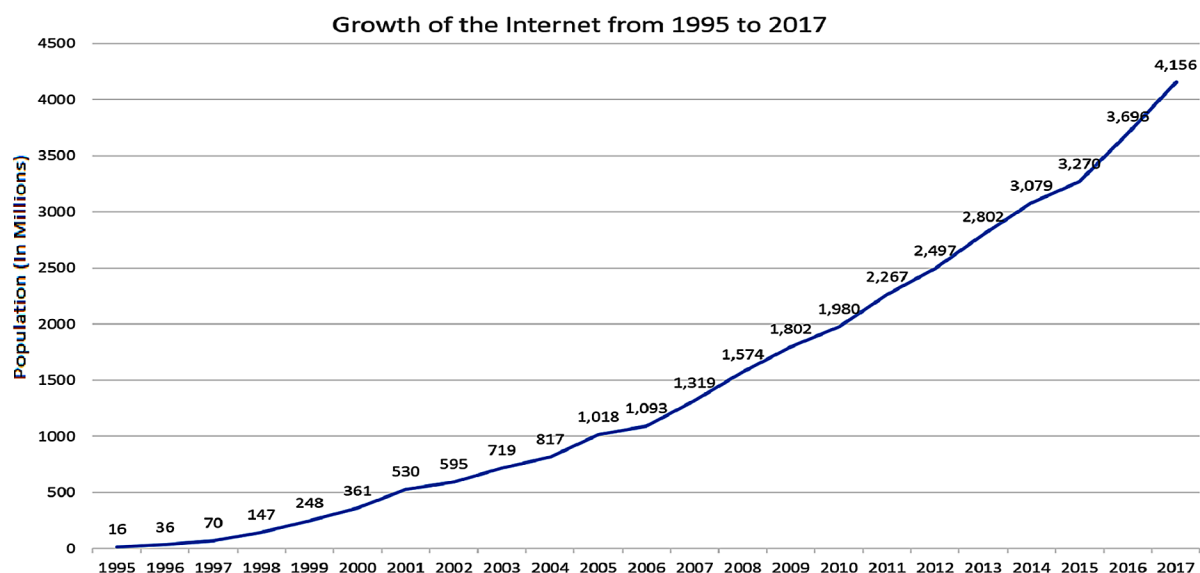
BACKGROUND

The Internet connection was available to general public in 1989 and the first ever website was launched in 1991. Today, there are more than a billion websites and the number of internet users is increasing with each passing day. Figure 1 shows exponential growth of the internet users from 1995 to 2017. There will be 6 billion internet users by 2022 which equals 75 percent of the estimated world population of 8 billion. This prevalent and dominant nature of computers and internet in our life has made cybercrimes more prominent (Morgan, 2017).

The first cyber attack took place in 1988. Morris Worm (named after its creator) infected thousands of computer systems and it took almost 72 hours to halt it. Nowadays these kinds of attack are frequent in numbers (Shackelford, 2018). The growth in importance of cyberspace across the globe has enabled vectors for, and broadens the scope of many existing forms of cyber-attacks. On one hand, cyberspace facilitates globalization of businesses and on the other, it has become a global platform for committing crimes. Individuals or more specifically cybercriminals from across the globe are using this environment to attack critical infrastructures, government and private businesses by stealing, compromising the integrity of, and destroying the data. It has created new marketplaces and even the trafficking and exploitation of human and gives a privilege for the creation and exchange of solicitation and sexual exploitation related materials (Emerging Trends In Global Cyber Crime, 2017). Cybercrimes are diverting from traditional to newly advanced crimes that can create the hoax in the world for example the Petya ransomware paralyzed the biggest container port in Mumbai, India; the cybercriminals breached the presidential election campaigns in France and USA (Cybersecurity Regained: Preparing to Face Cyber Attacks, 2017). Cybercriminals are fueled primarily by economic motives and non-economic motives. Crimes done with economic motives may include cheating, credit card fraud, money laundering, cryptojacking etc. Crimes done with non-economic motives may include cyberstalking, cyberbullying,

Figure 1. Growth of internet users from 1995 to 2017

Source: <https://www.internetworldstats.com>



cyberdefamation etc. In order to understand the world of cybercrime, there are terms which are required to be defined. Some of them are:

1. **Botnet:** Group of computers connected to internet which are compromised by bots for malicious intent, usually DDoS Attack.
2. **Computer Virus:** A malicious software loaded in a user's computer, when executed, has the capability to damage the files and replicate itself. In order to damage and infect other executables, it attaches itself to an existing program.
3. **Computer Worm:** A type of malware that spreads by replicating itself from computer to computer. It uses a network to spread itself due to inadequately protected computers and the servers on the network. It doesn't need a host program to run.
4. **Cyberbullying:** It is the use of cyberspace to bully or harass someone.
5. **Cyberstalking:** This occurs when internet is used to harass or frighten where the user is subjected to a plenty of online messages and emails.
6. **Cyberdefamation:** This occurs when defamation takes place using computers and/or internet.
7. **Distributed Denial of Service Attacks (DDoS Attacks):** They make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources.
8. **Identity Theft:** This cybercrime occurs when a criminal is misusing personal information after gaining access to it.
9. **Malware:** A malware is a computer software designed to disrupt, damage or gain access to computer or computer network.
10. **Phishing:** This cybercrime aims at using email messages to get personal information from users.
11. **Spyware:** Spyware is a type of malware installed on a user's computer often without his knowledge, designed to gain access to steal sensitive information or damage your computer.
12. **Spoofing:** It is a malicious practice in which a person or programs impersonates and attempts to gain unauthorized access to a user's system or information.
13. **Trojan:** A Trojan horse or Trojan is a type of malware which disguises users of its true intent. It is used to gain access to the target computer.

Focus of the Article: Emerging Trends in Cybercrime

According to Interpol “*New trends in cybercrime are emerging all the time, with an estimated cost to the global economy running to billions of dollars*”. In the past cybercrimes were committed mainly by small groups or individuals. Today, there are highly complex cyber criminals' organizations that have individuals from all around the world to commit crime at an unprecedented scale (Interpol). Cyber criminals on the web keep track of cyber security trends and react to them by modifying viruses, exploits and other methods to beat the safety nets. Traditional attacks are dependent on a lot of intermediary factors in the overall attack chain which is subject to detection by firewalls, antivirus, and intrusion detection systems. This has led attackers to use advance techniques to avoid detection and/or bypass defenses (Zimba, Wang, Mulenge, & Odongo, 2018).

There is a growing trend of highly targeted attacks, in which criminals manually break into a company computer, disable or evade internal security tools, and launch malware on whole networks of machines, all at once (SophosLabs 2019 Threat Report, 2018). Another growing trend is the use of cyber-attacks to target critical infrastructure and strategic industrial sectors that raise fears, in the worst case scenario, the attackers could trigger a breakdown of societal systems. Stuxnet malware attack is an example of

such attacks (Falliere, Murchu, & Chien, 2011). Emerging attacks are well thought-out and focus on new attack vectors and vulnerabilities enabled by technologies for example: exploiting vulnerabilities on smart devices to gain access to data and control systems. Not only this, cybercriminals are spending a lot of money for specific research to find exploits and vulnerabilities.

The cyberbullying has reached to a whole new level where harassed people are committing suicide. In 2017, there was a rumor of online game named BlueWhale or BlueWhale Challenge which challenged its participants/victims to do a series of tasks with the final task to commit suicide by beaching whale in the hand, caused unrest worldwide. According to Cyberbullying Research Center, between October 2016 and April 2017 there were 232,000 BlueWhale hashtags in Russia which the social networking site Vkontakte identified that bots (not real people) were using those hashtags, implying that the game started with fake news and eventually it went live (Patchin, 2017). Cybercrimes are not always new but they evolve in accordance with the opportunities presented online. Here are the some emerging areas of cybercrimes which are reshaping the traditional cybercrimes.

Crypto Mining: Cryptocurrencies popularity reached an all-time high when Bitcoin values increased by over 1300 percent and reached a record US \$ 19,783 per coin in 2017 at one point. They have become hot new investments for investors and fortune hunters. But they are not only ones interested in them. Cryptocurrencies have become a major point of interest for cyber criminals, as they present a perfect opportunity for them in various aspects (Sigler, 2018). There has been seen a major shift in cyberspace toward the use of cryptocurrencies for proceeds of cybercrime activities because they are easy to transfer and carry a low risk of catching the criminal(s) (Zimba, Wang, Mulenge, & Odongo, 2018).

Crypto mining, the process of generating the cryptocurrency, requires the use of computational power to solve complex mathematical equations as proof of work. It requires a lot of CPU resources. To overcome this issue, cybercriminals use crypto jacking which is running a mining script on someone else's machine without their knowledge or permission to illegally mine cryptocurrency. Crypto jacking has become an ideal venture for criminals because it is easy to deploy and safer to perform on target machines. Two most common attack approaches used by cyber criminals are crypto mining based on the web browser which leverages JavaScript, and installable binary crypto mining where the malware is running in memory (Zimba, Wang, Mulenge, & Odongo, 2018). High-traffic websites are the most popular choice for crypto mining operations, as a higher number of active users generate currency more quickly. Early in 2018, a malware known as Smominru was found to have compromised half a million machines for crypto mining (Sigler, 2018). In September 2018, the Economic Times (ET) revealed that Indian government websites were not spared this phenomenon, stating that widely-trusted Indian portals had been exploited by the crypto jacking menace (Christopher, 2018).

Advanced Social Engineering: Computer network security today maintains sufficient robustness and sometimes even automated vigilance experienced hackers are no longer seeking to replace social engineering but rather see it as an integral part (perhaps the most important part) of any successful toolkit for hackers (Mitnick & Simon, 2002). In fact, some observers now call social engineering "the highest form of hacking" (Greiner, 2006). Kaspersky Labs defines social engineering as a form of techniques employed by cyber criminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites (Kaspersky Lab).

It is a technique that distinguishes one variant of social engineering attack from another depending on the specific form of the attack as impersonation is an attempt to gather authentic information to gain access to a targeted network; third party authorization occurs when authentication details are stolen by or given to the third party; phishing emails are an attempt to trick the recipient into performing some action, usually clicking on malicious link or downloading an attachment, it tends to be the most diffi-

cult social engineering tactics to detect as sophisticated attackers can often send emails that look same to real ones; internal social engineering happens when a system administrator uses social engineering techniques against their own organizations to identify individuals who represent weak nodes in the network; reverse social engineering is said to occur when instead of attacker initiating contact with the victim, the reverse occurs i.e. the victim is tricked into initiating the contact themselves; automated social engineering attacks use botnets, algorithms and automated programs to perform many of the social engineering attacks that used to require skilled interaction between attacker and victim, and semantic attacks are an attempt to seek to deceive rather than directly attack a victim through the manipulation of object characteristics (Hatfield, 2017).

During the 2016 United States Presidential election, the chairman for Hilary Clinton's campaign John Podesta was sent an email that appeared to be legitimate Google Mail containing security warning caused due to suspicious activity involving someone attempting to log in to his account from Ukraine. The e-mail asked that Podesta change his password immediately and helpfully provided a link for him to do so. The campaign's IT help desk couldn't check the authenticity of the e-mail and they notified that he should change his password immediately which led to hacking of his account (CBS News, 2016).

Attacks on the IoT: According to Intel, there will be 200 billion smart devices or IoT devices by 2020. ABI has forecasted that more than 20 million connected cars will ship with built-in software-based security technology with 2020 and Spanish telecom provider Telefonica estimates that by 2020, 90 percent of cars will be online compared with just 2 percent in 2012. Gartner has predicted that more than half a billion wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearable include smart watches head-mounted displays, body-worn cameras, Bluetooth headsets and fitness monitors (Morgan, 2017).

David Wall speculated back in 2007 that the fourth generation of technology might be oscillating between completely virtual crime taking place in the virtual world or ambient crime (targeted at Ambient Intelligence, or Internet of Things), it is increasingly becoming apparent from above numbers that it will be the latter (Wall, 2007). Society is becoming more vulnerable due to introduction of autonomic devices and its move towards interconnecting everything by using internet as the medium; these vulnerabilities are bound to be exploited by criminals and terrorists. The interconnected advantages and accessibility involved in the IoT means that cyber criminals would likely be interested in ways to compromise this channel. Businesses will be more vulnerable to these attacks if they use IoT for security of building or any other back-end processes. The threat on IoT may even be to life as everything is getting smart from bulb to car, imagine the case when the criminals getting access to controls of support systems in hospital or taking control of connected cars on road. In 2016, the Mirai malware attack took advantages of vulnerabilities of IoT devices, infecting thousands of devices like unprotected webcams, TV networks and other smart devices. This allowed hackers to launch a DDoS attack (Internet Security Threat Report, 2017).

Other Crimes: Cyber criminals always find new and complex ways to commit crimes in order to achieve their objective which can be monetary gain or other reason. And getting hands on the sensitive data of big organization can be worth a fortune for attacker. So he tries to gain access to any organization's database that may contain sensitive information about their customers, employees or any Personally Identifiable Information (PII). **Data breach** is an incident where information is stolen or extracted without knowledge of system's owner. Data breaches are almost every day in the news. Technology giants such as Facebook and Yahoo have not been able to save themselves from data breaches. In 2014, 3 billion user profiles were compromised in Yahoo's data breach, largest in the history till date. According to reports, 4 billion data records of various kinds were stolen in 2016. In 2018, Facebook has been in the news for a high profile data leak. The data stolen from Facebook was being used by Cambridge

Analytica to manipulate the human behavior using techniques like artificial intelligence and machine learning. In November 2018 the hotel chain Marriott announced the massive data breach of its 500 million customers (Time, 2018). Figure 2 shows the biggest data breaches in the history.

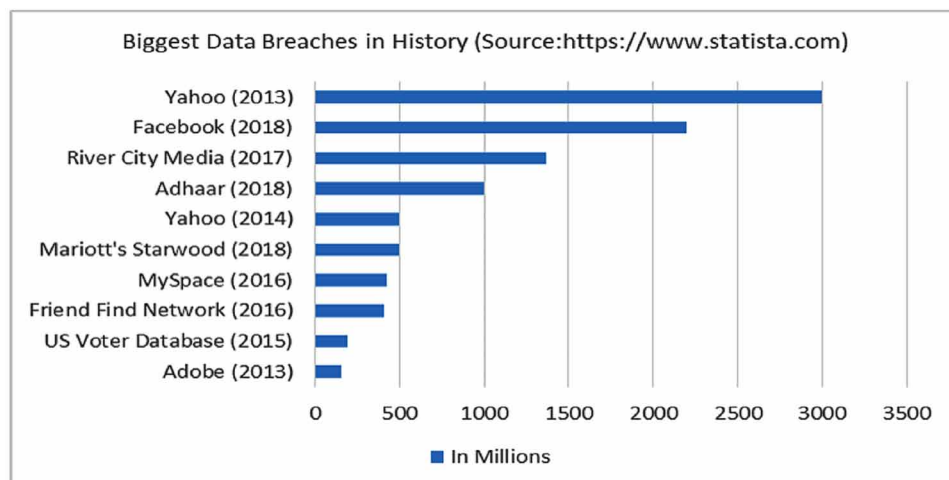
Digital wildfire is another cybercrime that is creating buzz globally. Digital wildfire can be defined as spreading of the misinformation rapidly over the internet. They can rip through public at breakneck speed and can cause social and economic unrest in the world. In 2018 Facebook disclosed that Russians with fake names used the social network to try to influence United States voters during the 2016 election by spreading false information. The Guardian has reported that the Russian president, Vladimir Putin, has spent more than £1 billion a year to for spreading fake news. In addition, there is troll factory (company set up in order to post comments and messages to influence people) based in St. Petersburg, Russia primarily for spreading fake information, sending spam messages and causing DDoS attacks (The Guardian, 2018).

The Evolution of Malware

Malware, the broad term for any type of malicious software that can harm computers, is a major problem. And it's getting bigger and worse, promising to poison everything from home appliances to national politics (The Evolution of Malware). A data infographic compiled by cyber security solutions firm RSA noted that one in every twenty malware attacks around the globe involves the use of ransomware (Emerging Trends In Global Cyber Crime, 2017), a type of malware in which the attacker encrypts the data and/ or blocks the computer access by the victim and demands money in return to restore functionality. There is a new emerging trend in malware: use of publically available and tested exploits like Eternal Series (developed by National Security Agency, USA) to create malware for increasing the chances of successful attack (SophosLabs 2019 Threat Report, 2018). One such example is Petya ransomware which uses Eternal Blue and Eternal Red exploit as a weapon to propagate in compromised machine network. Deploying malware on a multi-national scale is simple as WannaCry showed us (Emerging Trends In Global Cyber Crime, 2017). Today's malware are mostly machine-driven. But criminals are moving towards manually deployment of malwares to increase the chances of achieving their goal. The cyber

Figure 2. Biggest data breaches in history

Source: <https://www.statista.com>



criminals are also using *multi-intent* malware to attack target machines. Multi-intent malware starts by executing a malicious intent and once it has maximized the revenue from that channel, it moves onto another. It does this until it completes all the malicious intent it was programmed to execute. XBash is an example of multi-intent malware. It not only included ransomware, botnets and worms but also ability to reconnaissance (Darkreading, 2018).

As there is a greater degree of success to get hold on the ransomware attacks, the attackers are targeting to such victims and devices that have the capacity to pay greater sums and are new in the market and have security flaws, respectively (McAfee Labs 2018 Threats Predictions Report, 2017). A business will fall victim to a ransomware attack every 14 seconds by 2019 up from every 40 seconds in 2017. Ransomware attacks on healthcare organization are expected to quadruple by 2020 (Morgan, 2017). One such attack on the Dyn DNS provider brought internet to a pause, deranging tech giants like Twitter and Spotify amongst others (Cybersecurity Regained: Preparing to Face Cyber Attacks, 2017).

While malware that runs on the Windows operating system still outnumbers malware for any other platform (SophosLabs 2019 Threat Report, 2018), malwares are making their way from PCs to mobile phones as they have become an essential part of people's life and certainly contain a massive amount of personal information from photos to banking details. Users of mobile devices are subjected to malware integrated applications to their phones, tablets, or other devices with Android and iOS operating system. The most well-known is SMiShing, which tricks clients into uncovering individual data and passwords (Smishing - Text Messaging Scams). Malware's unpolished effectiveness implies its reach will keep on growing exponentially.

Impact of Cybercrimes

Main impact of cybercrimes are monetary losses. But there are other impacts which are not measurable but they can lead organizations to shut down. The stakes are higher as the organizations falling prey to cyber-attacks are at risk of reputational and as well as consumer loss.

Economic Impact: The 2017 Norton Cyber Security Insights Report disclosed that in the year 2016, 978 million consumers were affected by cybercrime and the total financial cost of cybercrime was US \$172 billion globally (2017 Norton Cyber Security Insights Report, 2017). An estimate put the economic impact at US \$445 billion worldwide, and about 15-20 percent of value is created by the internet. In many cases, the estimate on economic losses can be misleading. This is because too many companies still fail to quantify the losses related to cybercrime. In some cases, they are completely unaware that they are the victim of attack. Most numbers are based on a survey and loss estimates are based on raw assumptions of magnitude and effect. Cybercrime is more profitable than the global trade in marijuana, cocaine and heroin combined as cybercrime victims lose about US \$290 billion each year according to global estimates (Aiken, Mahon, Haughton, O'Neill, & O'Carroll, 2015). According to Center for Strategic and International Studies (CSIS) and McAfee report named Economic Impact of Cybercrime- No Slowing Down the global estimate suggests that as a percentage of global GDP, cybercrime cost the global economy 0.8 percent in 2017 (The Economic Impact of Cybercrime- No Slowing Down, 2018). The scale of the threat is expanding drastically: by 2021, the global cost of cyber security breaches will reach US \$6 trillion by some estimates, double the total for 2015 (Cybersecurity Regained: Preparing to Face Cyber Attacks, 2017).

Cybercrime is doing unmatched damage to both private and public enterprises and driving up IT security spending. Cybersecurity Ventures Report 2017 predicts 12-15 percent year-over-year cyber security market growth (Morgan, 2017). Today everyone has become highly dependent on computer and

networks for storing and preserving information, as a result, the risk of being subjected to cybercrime is huge. The CIA triads (Confidentiality Integrity Availability) of computer systems are continuously attacked by cybercriminals. According to surveys done in the past, 80 percent of the companies' surveyed acknowledged financial losses due to data breaches. The approximate number impacted was US \$450 million. As the economies are racing towards digitalization, they are exposed to all the threats posed by cybercriminals. Financial transactions are performed via the internet, payments are made by credit cards via the internet, and stocks are traded via the internet. Every fraud in such transactions, detrimentally affects the company's reputation and productivity thereby causing financial losses. Today in the era of globalization one region is dependent on another. Hence the disruption of financial market of one region could have a ripple effect in other regions (Saini, Rao, & Panda, 2012).

Impact on National Security: When it comes to national security, the impact of cybercrime can be huge. Almost every entity of a nation be it government, private organisations, individuals all depend on internet in some way or the other. The attack can affect an individual or an entire nation, whatever may be the case it would undermine the confidence of people for the government in motion.

Militaries of most of the countries rely heavily on advance computing with all almost all resources digitally connected, even the nuclear weapons. This could turn the prediction of cyberwar into reality. Cyberwar refers to the use of digital attacks like computer viruses and use of malicious codes by one country to disrupt the important computer systems or networks of another, with the aim of creating damage, death and destruction. It will see hackers using codes to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles (Ranger, 2018). It has potential to disable, damage and destroy military systems, space systems and can push back civilization decades back. In order to avert this disaster it is very important for nations to secure their digital space in a robust manner, thus securing the nation.

Impact on Consumers: Companies attacked by cyber criminals could have a huge impact on consumer trust. As the concept of e-business and e-commerce is dominating the market, more consumers are doing activities like shopping, banking etc. online. Visiting the concerned page which is subjected to cyber-attacks, discourage the consumer from using it on a long-term basis. As most of the consumers are unaware of the third party involvement (more specifically cyber criminals) in the crime, so they call the compromised site fraudulent. This makes consumer not only lose trust in the e-commerce but they altogether lose confidence in using the internet for various other purposes (Saini, Rao, & Panda, 2012). A survey revealed that 63 per cent people believe it's harder to stay safe online than in the real world (2016 Norton Cyber Security Insights Report, 2016).

SOLUTIONS TO PREVENT CYBERCRIMES

Cybercrimes continue to grow rapidly at an ever increasing pace. When one hears and reads about the range of cybercrimes out there, an individual might be tempted to stop using the internet entirely, but that is not the solution. Instead, it is better to be aware and take precautions to help protect against it. Some of the basic measures that can be employed at the grassroot level are by having proper awareness about the scams that exist on the World Wide Web and the precautions that need to be taken to avert them. This can be done by keeping oneself updated through internet by following cyber awareness websites and people who research in this domain.

It is often noticed that people become victims of such crimes by clicking on links that might pose to real but in reality are phishing links. These links ask for important credentials such as username, password or in many cases would download a malware into one's system, which can prove to be detrimental. So, it is very important to be cautious enough before clicking any link, especially when the link is from unknown sources. Also, due to ever evolving nature of security breaches it is very important for an individual to keep their system's operating system updated with latest security patches. Some of the basic things that can be done at the user level are firstly, using a firewall protection, it monitors the traffic between computer and the internet and filters the malicious requests beforehand to keep the intruders at bay. Secondly, strong passwords need to be used to protect confidential data, though it is easier to remember passwords like pet's name, birthdate, personal name but they can easily be cracked. Hence, it is important to use passwords which are at least 10 characters long and consist of combination of letters (Dell). It is even better to prefix a small sentence before the chosen password this would not only make it long enough but also make it difficult to crack. Thirdly, all personal/company data should be backed up to a secondary source to be safe in case of any data breach or ransomware attack.

Businesses can review and implement standards defined by the National Institute of Standards and Technology (NIST) framework, the European Union's General Data Protection Regulation (GDPR) or any other reputed organizations to ensure security from cyber-attacks. GDPR is the set of rules governing the security and privacy of personal data and NIST focuses on publishing standards for various industries in wide variety of areas.

The most alarming issue with cybercrimes is that they are borderless, without any territory. So, it becomes very important for countries to come together and form global organizations, facilitating them to work together in catching the culprit. Mere coming together of countries will not help, instead a multidimensional approach is required wherein, IT companies, financial institutions and law organizations work in unison to tackle these issues. Also, close cooperation between public and private players is of utmost importance given the enormous risks associated with global connectivity boom. Cyber Education - Hackers aren't the only ones who can gain power from information. By educating oneself about the types of scams that exist on the Internet and how to avert them, an individual is putting oneself a step ahead of the cybercriminals. Read up on the latest phishing scams and learn how to recognize a phishing attempt.

FUTURE RESEARCH DIRECTION IN CYBER CRIMES

With evolution of technology, cybercrimes have also evolved and increased the complications and risks associated with it. Every day there is a different type of attack on a vulnerability which needs to be addressed seriously. Hence, a lot needs to be done, especially in research and development sector to find solutions to the upcoming threats, in order to be future ready and avert any upcoming cyber disaster.

One of the major area that needs to be researched upon is that of artificial intelligence (AI). It has its own merit and demerits. On one hand, it can help the organizations to defend from cyber-attacks and on the other it can be used notoriously by cyber criminals to carry out malicious activities. In this era, cybercriminals are posing never ending threats to the cyber world with new and dangerous malware, botnets and viruses, in such a scenario solutions coming with AI are promising. Advances in machine learning technology mean that AI applications can automatically adapt to changes in threats and spot problems as they arise. The pattern detection algorithms, advanced analytics, and automated alerting systems make machine learning an effective tool to fight cybercriminals (Singh, 2018)

With innovation in technology everything around us is connected to internet be it refrigerators, air conditioners, wearables, mobile phones, vehicles, computers and what not. All these devices have an operating system or firmware, which if, accessed by a hacker can create a blunder. In order to curb this foreseen havoc, proper research needs to be done on how to secure these devices. Also, the root cause of most of the cyber-attacks is the malware hence, their analysis is essential .It requires proper virtualized lab environment to study its behavior so as to contain the intrusion and stop it before it does any damage.

CONCLUSION

This paper presents an overview of traditional and emerging cybercrimes around globe and explains their impact on economy, consumer and national security. This will help the society to understand the need of tackling the cybercrimes and the ways to safeguard themselves. Understanding the behavior of people behind the screens who are committing the cybercrimes, is not an easy task but it will definitely help to find out the ways to overcome the situation.

With boom in internet usage worldwide, the cybercrime, in realities, will be growing at similar pace to real world crimes within a short span of time. The fear of cybercrimes on cutting age technology is unbound and can do potential damage to the society. Due to borderless nature of these crimes it is important for countries to come together and form organizations that work in unison for proactive research in the cybercrime area and should develop new innovative international norms keeping in mind the dynamic nature of the field. Policy making and strong cyber laws are the ways to overcome these crimes. But most of the nations are yet to work on it. Widespread awareness amongst all sections of society will help to mitigate portion of the crime. Societies and government have a vital role to play in maintaining the healthy digital hygiene but the software giants and those with ability to stop frauds are the ones who can prevent the cybercrimes and help in preserving the consumer trust on using the cyberspace. There is still lot of research to be done in the in the ways to defeat the menace of cybercrime.

REFERENCES

2016 Norton Cyber Security Insights Report. (2016). Norton by Symantec.

2017 Norton Cyber Security Insights Report. (2017). Norton by Symantec.

Aiken, M., Mahon, C. M., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). *A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online.* Taylor & Francis.

CBS News. (2016). Retrieved from <https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/>

ChristopherN. (2018). Retrieved from ETRise: <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/hackers-mined-a-fortune-from-indian-websites/articleshow/65836088.cms>

Cybersecurity Regained: Preparing to Face Cyber Attacks. (2017). EY.

Darkreading. (2018a). Retrieved from CyberCrooks Diversify Business with Multi-Intent Malware: <https://www.darkreading.com/risk/cyber-crooks-diversify-business-with-multi-intent-malware-/a/d-id/1333249>

DarkReading. (2018b). Retrieved from DarkReading: <https://www.darkreading.com/endpoint/5-emerging-trends-in-cybercrime/a/d-id/1333363>

Dell. (n.d.). Retrieved from Dell: https://www.dell.com/downloads/ca/support/top_10_steps_to_protect_against_cybercrime_dell_en.pdf

Emerging Trends In Global Cyber Crime. (2017). Retrieved from Maryville University: <https://online.maryville.edu/blog/emerging-trends-in-global-cyber-crime/>

Falliere, N., Murchu, L. O., & Chien, E. (2011). *Stuxnet Dossier*. Symantec Security Response.

Global Cybersecurity Index (GCI). (2017). International Telecommunication Union.

Goodman, M. (2015). *Future Crimes: Everything Is Connected, Everyone Is Vulnerable And What We Can Do About It*. Penguin Random House.

Greiner, L. (2006). Hacking Your Network's Weakest Link. *netWorker Magazine*.

Hatfield, J. M. (2017). Social Engineering in Cybersecurity: The Evolution of a Concept. *Computers & Security*.

Internet Crime Report. (2017). Federal Bureau of Investigation.

Internet Security Threat Report. (2017). Symantec.

Interpol. (n.d.). Retrieved from <https://www.interpol.int/crime-areas/cybercrime/cybercrime>

Invading privacy: Cyber crimes on the rise. (2013). PwC.

Kaspersky Lab. (n.d.). Retrieved from <https://usa.kaspersky.com/resource-center/definitions/social-engineering>

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). *Advanced Social Engineering Attacks*. Elsevier.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on financial sector. Elsevier.

McAfee Labs 2018 Threats Predictions Report. (2017). McAfee.

Meeuwisse, R. (2017). *Cybersecurity For Beginners*. Cyber Simplicity Ltd.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception*. Academic Press.

Moitra, S. D. (2014). *Cybercrime: Towards an Assessment of its Nature and Impact*. Taylor & Francis.

Morgan, S. (2017). *2017 Cybercrime Report*. Cybersecurity Ventures, Herjavec Group.

Patchin, J. W. (2017, May 16). *Blue Whale Challenge*. Retrieved from Cyberbullying Research Center: <https://cyberbullying.org/blue-whale-challenge>

Ranger, S. (2018, December 4). *ZDNet*. Retrieved from ZDNet: <https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/>

Saini, H., Rao, Y. S., & Panda, T. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications*, 202-209.

Security Predictions for 2018 Paradigm Shifts. (2017, December 5). Retrieved from TrendMicro: <https://www.trendmicro.com>

Shackelford, S. (2018, November 5). *What the world's first cyber attack has taught us about cybersecurity*. Retrieved from World Economic Forum: <https://www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges>

Sigler, K. (2018). Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, 12-14.

Singh, A. (2018, June 13). *CXOtoday.com*. Retrieved from CXOtoday.com: <http://www.cxotoday.com/story/ai-is-the-future-of-cybersecurity/>

Smishing - Text Messaging Scams. (n.d.). Retrieved from Genisys: <https://www.genisyscu.org/files/genisys15/1/file/OnlineSecurity/SmishingTextScams.pdf>

SophosLabs 2019 Threat Report. (2018). Sophos.

The Economic Impact of Cybercrime- No Slowing Down. (2018). CSIS and McAfee.

The Evolution of Malware. (n.d.). Retrieved from WIRED: <https://www.wired.com/brandlab/2016/12/cylance-evolution-malware/>

The Global Risks Report 2018 (13th Edition). (2018). Academic Press.

The Guardian. (2018). Retrieved from <https://www.theguardian.com/world/2018/dec/05/eu-disinformation-war-russia-fake-news>

Time. (2018). Retrieved from <http://www.time.com/5467781/mariott-data-breach-information/>

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Whittaker, E., & Kowalski, R. M. (2015). *Cyberbullying Via Social Media*. Taylor & Francis.

Zimba, A., Wang, Z., Mulenge, M., & Odongo, N. H. (2018). Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. *Journal of Computer Information Systems*.

KEY TERMS AND DEFINITIONS

Artificial Intelligence: It is the area of computer science in which machines are created that have ability to think and learn like human.

Bot: It is a virtual robot created to automotive task both simple and repetitive.

Cyber: A broad term relating to or characteristic of the culture involving computers, information technology, and the internet.

Cybercrime: Crime done in or using cyberspace is called cybercrime.

Cyberspace: Cyberspace is the environment created by the links of tangible like a computer, intangible like application and services, and networks like the internet and communication.

Internet: It is a network of networks that connects millions of computers together globally. It is used for communication, entertainment, etc.

Internet of Things (IoT): IoT is a concept of connecting any device to the internet or other connected devices to send and receive data.

Machine Learning: It is the science of training the machine how to learn using algorithms and mathematical models to improve their performance.

Artificial Intelligence–Based Cybercrime

Bogdan Hoanca

University of Alaska, Anchorage, USA

Kenrick J. Mock

University of Alaska, Anchorage, USA

INTRODUCTION

The field of Artificial Intelligence (AI) has made swift progress in recent years, becoming much more pervasive in the lives of ordinary citizens. Many of the advances in AI have already led to exciting capabilities: intelligent agents on smartphones (Apple's Siri and Microsoft's Cortana), intelligent voice interaction devices in the home (Amazon's Echo) and countless interactive toys for children. Other upcoming advances are even more impactful, from self-driving cars to learning robots (Pinto & Gupta, 2015) and intelligent systems that automate the jobs of white-collar professionals. In fact, much has been written about the dangers of automation in terms of job losses (McKinsey & Company, 2017). Others fear even more wholesale threats to society, a dystopian future where super-intelligent robots enslave the relatively inferior humans (Barrat, 2013). Much of the AI-fear is driven by the prospects of super-intelligent AI agents (ASI – artificial superintelligence), agents so intelligent that humans will be as powerless against them as are ants against a human farmer. The literature on AI dangers focuses mostly on the unintentional dangers of AI developing into an ASI agent of destruction or danger, not because it develops a goal to kill us, but because it sees no problem in killing us in pursuit of a goal we designed it for (Bostrom, 2014).

Although fears of super-intelligent AI might be justified at some point, and although humanity needs to plan for the time and the manner in which ASI will be deployed (Bostrom, 2014), researchers have widely divergent views of when ASI agents will become reality (Walsh, 2018). Many experts are not even willing to speculate when ASI will arrive (Ford, 2018). In the meantime, a more immediate threat arises from not-yet-super-intelligent but already available AI: the ability of human attackers to use non-ASI systems to automate, enable and enhance cybercrime as we know it, as well as the ability to open totally new channels for cybercrime. Whether the long-term threat of ASI will materialize, the immediate threat of criminals using AI for cybercrime today needs to be considered – and is the focus of this article.

While focusing only on current AI capabilities, not on super-intelligent agents that are likely to emerge in the more distant future, we also focus only on intentional malicious uses of AI, not on dangers arising from unintentional consequences or on malfunction of AI systems. Neither do we discuss the threat of AI weapons, including autonomous or intelligent ones. Such systems are intended to create harm, and they can obviously be used for that purpose, whether by a legitimate authority or by a nefarious group.

Even after limiting the scope as described above, the range of capabilities of AI for achieving nefarious purposes is vast, at least as extensive if not more so than the range of capabilities for beneficial ones. Within this vast range of possibilities, we classify AI cybercrime into three general and loosely overlapping areas: using AI to commit cybercrime online, using AI via new cybercrime channels that

DOI: 10.4018/978-1-5225-9715-5.ch003

reach into physical space, and using AI or knowledge of AI to strike at the core of other AI systems, by corrupting data or algorithms. These are not three separated areas: they largely overlap, and the extent of their overlap will continue to increase. After providing a brief overview of AI history, the status of cybercrime in general, the article will delve into the three areas, highlighting the ways in which they interact presently as well as in the foreseeable future.

BACKGROUND

AI-based cybercrime is driven by two relentless forces: the development of AI, which has seen incredible strides in recent years, and the increasing volume and diversity of cybercrime, driven by more powerful technologies and more widespread use of the Internet. As background for the main topic of the article, this section will review recent trends in AI development as well as the status of cybercrime in general. The body of the article will focus on the convergence of AI and cybercrime.

Artificial Intelligence (AI)

A research field that emerged in 1956 at Dartmouth University, AI has undergone periods of excitement and growth, interspersed with periods of “AI winter” when excitement and funding dried out. The initial excitement was driven by the hope that major progress could be made swiftly in teaching computers to carry out intelligent activities. As researchers engaged with what they thought would be the most challenging tasks, the surprising discovery was that what was thought as most challenging would turn out to be easy, while some of the most effortless human skills proved most difficult to duplicate by computers. For example, computers were able to run highly complex calculations, to carry out abstract manipulations, create art (Charlesworth, 2018) and to get good at the most complex games, over time defeating the human world champions at backgammon (Berliner, 1980), chess (Weber, 1996) and most recently at Go (Hern, 2017). While the earlier successes were primarily examples of brute force computing overcoming human limited cognitive abilities, the Go victory was based on the system teaching itself to play by playing multiple games against itself (programmed with no strategy, but only with the rules of the game). To prove the point, after defeating the human champion, the Go playing AI proceeded to teach itself to play chess and defeated the chess program Stockfish 8 in a 100-game matchup (Silver, et al., 2017). Outside the field of games, AI systems are making similar progress, although at a somewhat slower pace: understanding images, natural language and achieving “common sense” turned out to be rather challenging for computers, even though such tasks were literally “child’s play” for humans.

Part of the problem with the initial failures in AI was that the approach was top-down: attempting to formalize and codify learning and knowledge, and to impart a corpus of this knowledge to the computer. This was overwhelming in terms of assembling such a corpus, as well as in terms of maintaining and debugging it. Starting in the twenty first century, the vast computing power made available by Moore’s Law, further made accessible by cloud computing and the Internet, revitalized some of the earlier attempts at using a bottom-up approach, where computers were given rules or examples and taught how to learn. Although neural networks with small numbers of neurons have been used almost from the earliest days of AI, the vast amounts of power and training data available have opened new possibilities when using much larger and deeper neural networks, an approach termed “deep learning.” While small networks are unable to improve in performance beyond a certain volume of training data, it became apparent that increasingly complex networks were able to continue to learn and to take advantage of the

huge training sets available. More than just winning at games, Deep Learning approaches using neural networks with multiple hidden layers (modeled after structures in the human brain) were successful in learning to classify videos and to use natural language (including language translation). Such systems even learned to play computer games with only receiving feedback on the outcome of the play, without being taught anything about the nature of the game (Mnih, et al., 2013). Furthermore, the ability to interact via natural language and to make some sense of context led to deployment of AI in consumer products and consumer-facing interfaces, from AI agents in smartphones (for example Apple's Siri or Microsoft's Cortana), AI-powered self-driving cars (Knight, 2017), and AI medical systems (Ng, 2016), just to give a few examples.

Among other uses more closely related to cybercrime, AI systems have been deployed in law enforcement, border control and in cybersecurity applications. For example, European Union researchers are developing a "deception detection" system to spot suspicious behavior at border crossings. Dubbed IBORDERCTRL (HomeBorderCtrl, 2018), the agent prompts users to upload travel documents and asks questions, while monitoring the traveler for suspicious behavior to provide a risk figure to the border guard for final processing. In law enforcement, VeriPol is an AI agent that can identify fake police statements using text analysis (Quijano-Sánchez, Liberatore, Camacho-Collados, & Camacho-Collados, 2018). In a real-life pilot test of the system, in only one week 64 cases of false robbery were detected and closed in two Spanish cities; for comparison, the human law enforcement agents typically detected and closed only 14 such cases on average. AI systems have also been developed to generate sketches of suspects that exceed the performance of human sketch artists (evofit, 2018). AI can even help solve previously unsolved crimes, by connecting the gunshot residue on a wound with particular types of guns or bullets in ways previously impossible to connect (Gallidabino, Barron, Weyermann, & Romolo, 2018).

Cybercrime

Traditional computer security is at increased risk today, with three quarters of the attacks motivated by financial gain (Verizon Enterprise, 2018). Cybercrime is driven by rogue nations, as well as by an organized crime industry that operates online by attacking organizations, to steal data for resale or for financial extortion (Ablon, Libicki, & Golay, 2014).

Attackers involved in cybercrime today rely mainly on rudimentary automation tools (running scripts). Attacks are carried out against known vulnerabilities, whether human or technological. For technological targets, attackers use lists of known vulnerabilities and run automated scanning tools to brute force attacks, going through the entire list of potential vulnerabilities (e.g., unpatched software or open ports). There is little intelligence in these scripts, and little if any human involvement until a vulnerability is found. Upon identifying a vulnerability, the script can execute code to take advantage of the vulnerability or can alert the human attacker to carry out additional steps.

For non-technology-related vulnerabilities, phishing and social engineering attacks focus on the weakest link in information security, the human element. Social engineering is the generic term for attacks that use psychological techniques that trick users into giving attackers access to protected resources. Using social engineering techniques involves pretending to be a person of authority or a person with a need to access information and convincing the target user to facilitate access. Alternatively, techniques involve the attacker pretending to verify the credentials of the target user (with the intention to learn these credentials and to use them later to access protected information). Phishing attacks are those where the request for credentials arrives in email form, either directing the user to submit credentials for verification on a website (or via email) or directing the target user to download or open malware. Malware

is a generic term for software that can be used as the attack vector, either by getting the target user to download it from a website or to open it as an email attachment. Malware is a pervasive problem, as attack vectors have become more powerful, more available and easier to deploy. For example, ransomware is a particularly concerning type of malware that takes over the user's data, encrypts it and requests the user to make a ransom payment to gain access to the decryption key. The threat can become even greater when combined with AI, as we detail in the body of this article.

In a perverse asymmetry, it is much easier to attack than to defend an organization. The 2018 Data Breach Investigations Report (Verizon Enterprise, 2018) finds that of the breaches reported 87% took minutes or less to complete but 68% took more than one month to discover.

Although the focus of this article is on AI-supported cybercrime from the standpoint of an attacker, AI can also be used from the perspective of defense. Many companies are utilizing AI and machine learning to detect threats and warn the user. For example, Microsoft's Defender software uses multiple algorithms and training sets to provide defense in depth in the event an algorithm is cracked. (Giles, 2018). A challenge that arises is to avoid the problem of false positives; too many will render the system unusable. While algorithms can often be tuned to minimize false positives as identified by its ROC curve, the result is a lower number of true positives. Even for this problem, AI may help find a solution. Recurrent neural networks have been demonstrated to model SQL injection attacks that learn, iterate, and adapt from false positives to reduce future errors (Wallarm, 2018).

AI-supported cybercrime has the potential to transcend all the factors that limit the scale of today's cybercrime. AI will augment, enhance and make more difficult to track the attacks.

Phishing Attacks

Phishing attacks, a type of social engineering attacks, are based on carefully researching weak spots of people and organizations, then customizing targeted attacks for these weak spots. According to an industry report, attackers created an average of 1.4 million phishing websites a month in 2017 and launched phishing attacks against 63% of the organizations surveyed for the report (Webroot, 2017).

Phishing attacks fall in two categories: mass phishing and spear phishing. Mass phishing attacks rely on sending to many users email messages, using easy to spot telltale signs: poor spelling, rather primitive formatting, relatively easy to spot fake logos and links. These telltale signs are deliberately used to elicit responses only from users with the lowest awareness of cybersecurity issues. By falling prey to such blatantly obvious lures, respondents signal that they are likely to engage with the attacker with little ability to resist, and that they are likely to provide the information the attacker is looking for. Given that most email users are at least somewhat aware of phishing threats, the telltale signs of typical phishing attacks lead to low response rates, which is acceptable and even desirable for the attacker, because the attacker lacks the capacity to engage with large numbers of respondents anyway; instead, attackers prefer to engage only with the few respondents who are most likely to fall prey to the attack. For automated phishing attacks, as described below, such considerations do not necessarily apply.

In contrast, spear phishing attacks are sophisticated and highly-targeted to carefully selected users, involving considerable prior research on the target individual, on the organization, the social networking profile and on any other relevant connections to the target user. Experts estimate that spear phishing emails are the tool of choice for 91% of the most qualified attackers (Morgan, 2017). A well-trained attacker takes only minutes to get into a target system, but this speed is based on countless hours of prior preparation and research (DeSot, 2017). This considerable time investment required on the part of the attacker clearly limits the number of victims an attacker can target; the investment of time is justified if

the target is a key gatekeeper for the information the attacker is seeking. In some cases, the respondents from the mass phishing attacks can become the targets of spear phishing attacks, or the information from a mass phishing attack can be used to identify and research other users as targets of spear phishing.

Automated Phishing Attacks

As early as 2015 experts estimated that most cyber-attacks are automated (Goodman, 2015), although attacks still require human involvement beyond a certain stage. For example, mass phishing attacks can be fully automated: the attacker designs the email message, purchases or harvests a list of email addresses for recipients, sets up a landing website where victims will be asked to verify (provide) their credentials, and sets up a database on the back end of the website, where the credentials will be stored. Phishing websites typically have a short lifetime, as they are discovered by information security professionals and blacklisted or targeted by white hat hacking counterattacks. Thus, the attacker has only a limited window to harvest credentials, but the process requires no human interaction once the site is set up. There are even tools available on hacker websites that will automate the entire process, starting with the generation of the email message, the setting up of the database and website and the collection of credentials. In contrast, spear phishing attacks are more difficult to automate. Beyond just collecting credentials, spear phishing attacks are intended to allow more comprehensive access into protected systems. After gaining access to valid user credentials, the attacker will actively use the system, for example syphoning data or installing additional tools to facilitate deeper access into the system. A recent trend is to install bitcoin mining software on breached systems, which makes it much easier to monetize a successful attack.

Cybercrime is a vast and growing field, and this introduction provides only the top-level highlights. For more information, there are many good books and papers that provide additional background. Next, the body of this article focuses on how AI is already able to enhance cybercrime.

ARTIFICIAL INTELLIGENCE-BASED CYBERCRIME

Autonomous AI agents with the initiative, motivation and the capabilities to attack humans would be the holy grail for attackers, but such agents are not likely to be developed soon. On the other hand, other simpler AI tools are already available, and they are likely being used by cybercriminals to enhance the efficiency of their attacks, to develop new attack channels or to strike at the core of data and algorithms that are used by legitimate AI. A recent report anticipates that AI will enable attacks that are “especially effective, finely targeted, difficult to attribute, and likely to exploit vulnerabilities in AI systems” (Brundage, et al., 2018). A survey of more than 1200 security executives worldwide (Thales eSecurity, 2018) found that while 64% of respondents view AI as a helper in achieving cybersecurity, 43% view the malicious uses of AI as concerning (respondents could select either or both views).

Although it is difficult to conclude when AI has been used in an attack, in an informal survey of 100 attendees of Black Hat USA 2017 62% of respondents anticipated that AI would be used for offensive purposes in the next year (The Cylance Team, 2017).

The core of this article presents examples and countermeasures for three types of cybercrime outlined in the introduction: using AI to commit cybercrime online, using AI via new channels that reach into physical space, and using AI or knowledge of AI to strike at the core of other AI systems, by corrupting data or algorithms.

Using AI to Commit Cybercrime Online

1

As mentioned before, the capabilities and the scale of attacks is currently limited by the abilities of attackers to handle either human or technological vulnerabilities. With the aid of smart AI tools, attackers will be able to identify, profile and interact with more potential victims, will gain access to attack vectors that are more credible (and more successful against their victims) and will carry out attacks that are harder to detect.

Using AI Will Enable Attackers to Use Social Engineering to Identify and Profile More Victims

Successful attacks require considerable amounts of research, in particular for spear phishing: to identify potential victims, to research the target for vulnerabilities and to design attack vectors that are most likely to succeed. Using data mining tools and techniques, attackers could use AI to automate the collection of information that could support social engineering attacks. Such uses of AI are already taking place, according to Deepak Dutt, the CEO of a mobile security startup quoted in Gizmodo (Dvorsky, 2017): AI tools are used to mine public data repositories, to monitor email messages and create personalized responses for social engineering.

Using AI Will Enable Attackers to Handle More Victims

For attacks that require human interaction, the attacker is limited in the number of victims it can handle at any given time. When using AI tools to automate the handling of user responses, many more victims can be handled at a given time. Using technologies already available, almost anybody can put together a chatbot in minutes (Ingraham, 2017); with such a tool, social engineers can then expand the capabilities of automated attacks, using the AI tool to engage the victim while posing as a human (Wasserman, 2018). Without a chatbot, if the user responds to the original email with a question or a concern rather than simply providing the credentials requested, the attacker has to engage one-on-one with the user to pursue the potential victim. When using a chatbot, the AI can handle simple inquiries and engage the user, with the hope of ultimately eliciting the credentials (Gambhir, 2017). The range of interaction for chatbots is currently rather limited, but the capabilities of AI are evolving and expanding continuously. Moreover, what such AI tools lack in sophistication they make up in volume and reach. Attacks can be launched via text (email) or voice (by phone). Ironically, a similar approach can be used to thwart phishing attackers, by getting the attackers to engage with a chatbot that will waste their time.

Using AI Will Make Attacks More Effective

Using AI can make phishing URLs more credible (Bahnsen, Torroledo, Camacho, & Villegas, 2018). Using Deep Neural Networks technologies trained on a database of more than a million phishing URLs, researchers were able to improve the efficiency of the URLs, making them less likely to be detected by defensive tools. The AI tool increased the effectiveness of two threat actors, from 0.69% to 20.9% and from 4.91% to 36.28%, respectively.

An older paper on training AI to carry out spear phishing attacks (Seymour & Tully, 2016) reported success rates of 30-66%, comparable with the 45% success rates of manual human spear phishing attacks. A journalist who tried to match forces with the AI spear phishing tool had to concede defeat: he averaged only one tweet per minute, with a response rate of 38%, while the AI agent generated six times as many tweets, with a similar response rate of 34% (Brewster, 2016).

Technologies that entice people to act are primarily developed for marketing purposes; like any tools, once developed they can be used for the intended purpose or coopted for more nefarious ones. Companies already see AI as a powerful tool to customize ads to maximize the response from potential consumers (Fati, 2016). The marketing approach uses feedback from the consumer's actions to fine-tune the marketing campaigns to further increase the effectiveness of the marketing message; using the same approach can use AI to fine-tune an attack vector to make it more effective. In the same way A/B testing is used to improve human response to marketing messages, AI can use A/B testing to increase the response rate to social engineering attacks well beyond improving the efficiency of phishing URLs. Ultimately, both the marketing campaign and the phishing campaign exploit the same human weaknesses and heuristics.

Another way AI can enhance the effectiveness of phishing is by allowing attackers to better impersonate others. Without AI, attackers build a credible persona, posing as a helpless customer or a vendor in need of special access on a short notice, but have a difficult time impersonating somebody known to the target. They can try to impersonate via email (spoofing the sender address) or via another channel where they are not easily recognized (faking somebody's voice on the phone). On the other hand, AI techniques already enable attackers to impersonate specific individuals, some who might be well-known by the victim, using much more impactful video or audio channels.

Deep learning techniques have been shown to deliver realistic computer-based impersonation through audio and video. Using samples of audio or video from a human target A and a video of another human B, machine learning is able to extract the key features of the target A and synthetically alter the audio and video of B to generate a realistic-looking video of A (dubbed a "deepfake"). Such audio and video deepfakes have already been the subject of "fake news" in which politicians appear to be making statements they did not actually make (Feathers, 2018), or celebrities appearing to act in pornographic videos (Bloomberg, 2018). While many concerns have been voiced about using deepfake videos for political or blackmail purposes (Chesney & Citron, 2019), the same technique can be used to create a Skype video of the victim's boss or to imitate the boss's voice in a voicemail. Standard procedures involve close screening of unexpected visitors on company premises, but most employees in any organization would gladly accommodate the visitors upon receiving a Skype or telephone call from someone who looks and sounds like their boss.

So far, AI tools that create deepfake videos are still expensive, which limits their use. The actual rendering of the person impersonated is convincing, yet not foolproof. Videos that have convinced many online viewers can be identified as fake only by experts, for example by evaluating the blinking behavior (Li, Chang, & Lyu, 2018). On the other hand, as AI tools get better at using natural blinking, detecting such fake videos will become increasingly more difficult even for experts.

One final way to make attacks more effective is to use AI to make intelligent scanners for technological vulnerabilities. We described earlier how attackers use brute force to test systems against lists of known vulnerabilities. Using AI, attackers will be able to program the AI to test for new vulnerabilities, for example using techniques from genetic programming.

Using AI Will Make Malware More Difficult to Detect

Today, malware attempts to obfuscate itself and may undergo mutations to hide itself from detection by virus scanners. AI-based malware has the potential to conceal itself in an intelligent manner, making it almost impossible to detect until its payload has been triggered. An IBM prototype, DeepLocker, has been developed to demonstrate this type of attack by hiding ransomware until activated by the face of a specific person (Stoecklin, 2018). Moreover, finding exploits to break into a system can also be enhanced by AI. In 2016, Carnegie Mellon's Mayhem AI won the DARPA Cyber Grand Challenge which involved automated scanning and attacking of adversary systems. Not surprisingly, the best defense against attack AI systems is to use defensive AI that can automatically detect, self-patch, and recover from attacks (Avgerinos, 2018).

Another example of AI helping make attacks more difficult to detect is in money laundering. Money laundering online can involve something as simple as multiple transfers of funds among many bank accounts, shuffling the money and making its source difficult to retrace. When using AI to control such schemes, it is possible to scale the shuffling until it becomes truly impossible to unwind. An actual case involved 250 accounts with money transferred among them (Patterson, 2018). It is already possible to manually set up a network of such transfers, but, using AI, the attacker can dynamically change the pattern of transfers, as well as learn from experience.

Using AI via New Cybercrime Channels that Reach Into Physical Space

Another class of cybercrime enabled by AI tools is to use the tool as a channel for new types of attacks. Any new technology creates new crime channels, maybe not surprising in retrospect, but surprising the first time. For example, a casino was breached via an Internet-connected thermostat in its gigantic fish tank (Clifford, 2018). Although not a case of AI-mediated cybercrime, this is an example of a crime channel that did not exist before the advent of the Internet of Things. AI will enable other surprising types of attacks that will only be considered when the technology to enable them will become available.

There are already reports of attackers using voice commands to get devices to unlock front doors of homes (Tilley, 2017). Similarly, personal assistant agents can be accessed via voice by an attacker on computers that are locked, for example to install malicious software (Kovacs, 2018). Since voice interaction devices are designed primarily for convenience, they are similar to the ideal victims of social engineering: primed to serve and accommodate, rather than question and protect. Current generations of voice interaction devices are not designed to recognize individual voices, but only to recognize and execute commands. As such, an attacker may ask a device to unlock the front door of a home they are breaking into, or may place an order for expensive merchandise with the intention of stealing it once it is delivered on the doorstep. Some attacks can even be targeted to a voice interaction device, but cannot be heard by nearby humans (Smith, 2018). An audio stream that appears innocuous to a human listener could in fact instruct the device to place an order or to execute a malicious action. This type of attack is part of the more general attacks on AI algorithms we describe in the next section. Until vendors will offer systems designed with security in mind, the designs focused only on convenience leave massive vulnerabilities in place.

Another type of attack channel is to use AI to generate counterintuitive artifacts in the physical world. For example, researchers have shown that it is possible to produce synthetic fingerprint templates that would match multiple users in a database (Bontrager, Roy, Togelius, Memon, & Ross, 2018). In general,

such attacks involve reverse engineering the AI recognition function. Attack AI systems called Generative Adversarial Networks (GANs) involve two systems, one that generates patterns and one that discriminates (evaluates) patterns, providing feedback on a measure of goodness of the patterns. The generator starts initially with random noise, then modifies the design via feedback from the discriminator system. Over time, using the feedback from the discriminator system, the generator can converge to producing patterns that are recognized as “good” by the discriminator. Both systems are programmed to co-evolve, making sure that as the generator improves in its ability to create more realistic patterns the discriminator becomes stricter in its evaluation process. In the earlier example, researchers used GANs to synthetically generate DeepMasterPrints, fingerprint patterns that can match a large number of user fingerprints in a database. Without attempting to match a particular user’s fingerprints, the system attempts to create fingerprint templates that look realistic and that match many users. Such DeepMasterPrints were shown to match 23% of users in a dataset at false match rate of 0.1% and a whopping 77% of users when the false match rate was 1% (Bontrager, Roy, Togelius, Memon, & Ross, 2018). For the actual attack using the synthetic pattern, a fingerprint replica could be created and used to gain access to a device with a fingerprint reader, with no knowledge of the actual fingerprint that is intended to unlock the device, the equivalent of a biometric master key.

Yet another type of physical attack using AI is to program or reprogram autonomous devices for malicious purposes. Such autonomous devices could include self-driving cars, for example to harm a given passenger or to harm a target pedestrian encountered during a trip. Autonomous drones owned by the attacker could be programmed and loaded with explosives, targeting a particular victim, or they could be hijacked from the fleet of a delivery organization and used for similar purposes. In 2016 a security researcher demonstrated how a professional drone could be hijacked remotely by exploiting the lack of encryption between the drone and controller (Rodday, 2016). Finally, robots, either in a household or in an industrial setting, can be used for corporate sabotage (Brundage, et al., 2018). Cleaning robots make up a majority of the number of robots worldwide, and they could be loaded with explosives or otherwise rigged to attack a human target.

Using AI or Knowledge of AI to Strike at the Core of Other AI Systems

The third type of cybercrime described in this article targets data and algorithms. The fingerprint attack discussed earlier is an example of using AI to attack at the algorithm level. An attack at the data level could involve stealing user data internal to the AI. For example, voice interactive devices that listen for commands can also record sounds, save them and possibly send them to third parties. In one case, a recording of a husband and wife conversation was sent (apparently thanks to a bug in the AI) to a person on their contact list (Zhou, 2018). More deliberately, an attacker could set the device to record such conversations, to be retrieved later and mined for data.

More attacks have been reported on the algorithm side than for data. For example, an image recognition system could be presented with an image crafted to look like a panda to a human observer, but to be recognized by AI as a car (Polyakov, 2018). The introduction of objects that were not encountered together in the AI training set can have strange and devastating effects on the accuracy of image recognition, with global and shift-variant effects (Rosenfeld, Zemel, & Tsotsos, 2018). For example, introducing an object in an area of the image affects the recognition of objects far away from the introduced object. Proximity of objects not typically found together can result in shift-dependent artifacts (an image featuring only a keyboard and a hot dog can be recognized as a dog, a teddy bear or a person in different areas of the

image, depending on the relative location of the two objects). In another adversarial attack, images showing widely different scenes (school bus, dog, pagoda, nature scenes) are modified only slightly, but the visually indistinguishable new images are all recognized as showing an ostrich (Szegedy, et al., 2014). In another paper, researchers added a noise background to a panda image that was initially recognized as such by the AI with 53% confidence. The modified image is indistinguishable from the original for the human observers, yet AI recognized it with much higher (99.3%) confidence, this time as a gibbon (Goodfellow, Shlens, & Szegedy, 2015). Finally, images that make no sense to human observers can be designed to be recognized with high confidence by deep learning systems (Nguyen, Yosinski, & Clune, 2015). Whether such image recognition systems are used for security (face recognition) or for another type of application, attacks on the algorithm can allow criminals to hijack the system by injecting noise, adding unexpected objects in the image frame or adding special markers to change the recognition process.

For face recognition applications, AI has been shown to enable attacks, using face markings or image transformations that would be classified correctly by human observers, but that would confuse deep learning algorithms. At the same time, AI tools are starting to identify such modified images, with the goal to increase the robustness of the recognition (Goswami, Ratha, Agarwal, Singh, & Vatsa, 2018). A similar technique might be applicable to the other attack vectors described in this section.

Modifying objects in the physical world (using stickers or markings) can also lead to faulty recognition, for example applying tape markings to a Stop sign can lead to it being recognized as a Speed Limit 45 mph sign (Eykholt, et al., 2018). Such attacks could induce a self-driving car to crash into oncoming traffic, as it speeds past the stop sign, rather than giving right of way. Attacks on speech-to-text translation systems can take any given sound clip (speech or non-speech) and optimize it into an adversarial input that is 99.9% similar to the original sound clip, but that is recognized as any given (different) target phrase. This is similar to what we described for attacks on the voice-interaction devices in the previous section. For example, an AI-crafted phrase that sounds to a human “without the dataset the article is useless” is recognized by speech recognition AI as “okay Google browse to evil dot com” and a brief AI noise-enhanced clip from Bach’s Cello Suite #1 (no speech) is recognized by speech recognition AI as “speech can be embedded in music” (Carlini & Wagner, 2018).

Adversarial attacks on reading comprehension systems have been shown to greatly reduce the accuracy of the AI, from an average of 75% to less than half (Jia & Liang, 2017). When attackers used grammatically incorrect words, the accuracy plummeted to 7%. Such attacks, whether using video, text or some other type of media, could hijack an algorithm to make it serve the purposes of the attackers, instead of its original functionality. In all the results discussed above, the adversarial input is optimized to create maximum error in the recognition system with minimum change in the input to the system. Such approaches are so called “white box,” because they require access to the recognition system, with intimate knowledge of how it is built and trained, as well as time to train and optimize the attack. This set of conditions might be available to attackers when systems use algorithms that are open source, widely available online.

FUTURE RESEARCH DIRECTIONS

As happened in the early history of the Internet, which was designed for a small group of technically savvy people who trusted each other, AI tools are currently designed for convenience and flexibility. Security is an afterthought if at all a consideration, and vendors focus on only two goals: convenience for the user and flexibility in accepting voice variations with age, health or different accents. Given how

difficult it is to retrofit security on the open architecture of the Internet, designers of AI tools should take heed and incorporate cybersecurity considerations early on. Additionally, “transparent AI” that allow the user to see how AI linked an input to an output will help debug some of the algorithm attacks on AI.

An interesting wrinkle will arise in correcting the behavior of AI, when needed. Some researchers advocate that when ASI agents become conscious they will gain rights like conscious humans: this will raise ethical issues about “turning off” or even “reprogramming” a conscious ASI (Bostrom, 2014). Some researchers even go as far as advocating for a mental health approach to “treating” misbehaving AI (Behzadan, Munir, & Yampolskiy, 2018). Other researchers are advocating a governmental agency to coordinate and eventually regulate AI, attracting AI practitioners to civil service, identifying relevant policy issues and even paving the way to international AI governance (Clough, 2018). Even when fighting an adversarial AI system, the question will remain on how to defeat it humanely if it is conscious.

AI learning is not robust to changes. For example, an AI system was able to learn to play one of the early computer games, Breakout, quite well, but the performance plummeted even for a small change that offset the paddle by a few pixels (Kansky, et al., 2017). As such, AI could be trained efficiently to attack a specific target, but would be difficult to train against a variety of attackers. On the other hand, such weaknesses in AI could be used to defend against AI-backed attacks, by slightly changing the landscape where the attack takes place.

CONCLUSION

There are strong voices urging humanity to plan for when super intelligent AI might turn against us. In the meantime, a more urgent need is to understand and respond to dangers from not-yet-super-intelligent AI that is used as a tool by malicious attackers. As Pedro Domingos feared, “[p]eople worry that computers will get too smart and take over the world, but the real problem is that they’re too stupid and they’ve already taken over the world” (Domingos, 2018). Given the financial payoff of cybercrime, the scale on which both rogue states and organized crime use cybercrime, it is a matter of time until AI becomes a tool of choice supporting criminal activities. Although this article describes the state of the art, technology evolves very fast, and attacks vectors will change from what is described in this article. It is nonetheless imperative for security professionals to be aware of the role of AI in cybercrime, of ways to defend against it, and of ways in which it will change their profession.

REFERENCES

- Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data*. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf
- Amazon. (2018). *Alexa - Amazon Devices - Amazon Official Site*. Retrieved from Amazon Official Site: <https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011>
- Avgerinos, T. B., Brumley, D., Davis, J., Goulden, R., Nighswander, T., Rebert, A., & Williamson, N. (2018). The Mayhem Cyber Reasoning System. *IEEE Security and Privacy*, 16(2), 52–60. doi:10.1109/MSP.2018.1870873

Bahnsen, A. C., Torroledo, I., Camacho, L. D., & Villegas, S. (2018). DeepPhish: Simulating Malicious AI. *Black Hat Europe*. Retrieved from https://albahnsen.com/wp-content/uploads/2018/05/deepphish-simulating-malicious-ai_submitted.pdf

Barrat, J. (2013). *Our Final Invention: Artificial Intelligence and the End of the Human Era*. Thomas Dunne Books.

Behzadan, V., Munir, A., & Yampolskiy, R. V. (2018). A Psychopathological Approach to Safety Engineering in AI and AGI. In *Computer Safety, Reliability, and Security. SAFECOMP 2018*. Cham: Springer. doi:10.1007/978-3-319-99229-7_46

Berliner, H. J. (1980). Backgammon Computer Program Beats World Champion. *Artificial Intelligence*, 14(2), 205–220. doi:10.1016/0004-3702(80)90041-7

Bloomberg. (2018, September 11). *How Faking Videos Became Easy -- And Why That's So Scary*. Retrieved from <http://fortune.com/2018/09/11/deep-fakes-obama-video/>

Bontrager, P., Roy, A., Togelius, J., Memon, N., & Ross, A. (2018). *DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution*. eprint arXiv:1705.07386

Bostrom, N. (2014). *Superintelligence*. Oxford, UK: Oxford University Press.

Brewster, T. (2016, July 25). Who's Better At Phishing Twitter, Me Or Artificial. *Forbes*.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., . . . Héigearthaigh, S. Ó. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute.

Carlini, N., & Wagner, D. (2018). *Audio Adversarial Examples: Targeted Attacks on Speech-to-Text*. arXiv:1801.01944

Charlesworth, J. (2018, September 10). *AI can produce pictures, but can it create art for itself?* Retrieved from CNN News: <https://www.cnn.com/style/article/artificial-intelligence-ai-art/index.html>

Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107.

Clifford, C. (2018, August 7). *How billion-dollar start-up Darktrace is fighting cybercrime with A.I.* Retrieved from CNBC News: <https://www.cnbc.com/2018/08/07/billion-dollar-start-up-darktrace-is-fighting-cybercrime-with-ai.html>

Clough, R. (2018). *The Inevitability of AI Law & Policy: Preparing Government for the Era of Autonomous Machines*. Public Knowledge. Retrieved from <https://www.publicknowledge.org/documents/the-inevitability-of-ai-law-policy-preparing-government-for-the-era-of-autonomous-machines/>

DeSot, T. (2017, January 13). *The Sorry State Of Cybersecurity Awareness Training*. Retrieved from Dark Reading: <https://www.darkreading.com/vulnerabilities---threats/the-sorry-state-of-cybersecurity-awareness-training/a/d-id/1327862>

Domingos, P. (2018). *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. Basic Books.

Dvorsky, G. (2017, September 11). *Hackers Have Already Started to Weaponize Artificial Intelligence*. Gizmodo.

evofit. (2018, 12 11). *Evolving Facial Composite Imaging*. Retrieved from <https://evofit.co.uk/>

Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., & Song, D. (2018). *Robust Physical-World Attacks on Deep Learning Models*. Computer Vision and Pattern Recognition.

Fati, M. (2016, August 23). *New artificial intelligence technology only delivers ads that actually change consumer opinion*. Retrieved from UK Tech News: https://www.uktech.news/press_release/new-artificial-intelligence-technology-delivers-ads-actually-change-consumer-opinion

Feathers, T. (2018, November 3). Deepfakes: the next threat to our elections? *New Hampshire Union Leader*. Retrieved from http://www.unionleader.com/news/politics/deepfakes-the-next-threat-to-our-elections/article_048c1795-7e51-51ad-8ce2-8b8121eedf15.html

Ford, M. (2018). *Architects of Intelligence: The truth about AI from the people building it*. Packt Publishing.

Gallidabino, M. D., Barron, L. P., Weyermann, C., & Romolo, F. S. (2018). Quantitative profile–profile relationship (QPPR) modelling: A novel machine learning approach to predict and associate chemical characteristics of unspent ammunition from gunshot residue (GSR). *Analyst (London)*. doi:10.1039/c8an01841c

Gambhir, S. (2017, May 31). Chatbots: Opportunity and threat. *ComputerWorld*. Retrieved from <https://www.computerworld.com.au/article/620035/chatbots-opportunity-threat/>

Ganti, V. (2018, June). The Role of Artificial Intelligence in Cybersecurity. *BizTech Magazine*.

Giles, M. (2018, August 11). *AI for cybersecurity is a hot new thing—and a dangerous gamble*. Retrieved from Technology Review: <https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/>

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). *Explaining and Harnessing Adversarial Examples*. eprint arXiv:1412.6572v3

Goodman, M. (2015). *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. Doubleday.

Goswami, G., Ratha, N., Agarwal, A., Singh, R., & Vatsa, M. (2018). *Unravelling Robustness of Deep Learning based Face Recognition Against Adversarial Attacks*. eprint arXiv: 1803.00401v1

Hern, A. (2017, May 25). Google's Go-playing AI still undefeated with victory over world number one. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2017/may/25/alphago-google-ai-victory-world-go-number-one-china-ke-jie>

HomeBorderCtrl. (2018). Retrieved from <https://www.iborderctrl.eu/>

Ingraham, N. (2017, March 12). Building your own chatbot is a lot easier than you'd expect. *Engadget*. Retrieved from <https://www.engadget.com/2017/03/12/build-your-own-chatbot-hands-on/>

Jia, R., & Liang, P. (2017). Adversarial Examples for Evaluating Reading Comprehension Systems. *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing* (pp. 2021-2031). Copenhagen, Denmark: Association for Computational Linguistics. 10.18653/v1/D17-1215

- Kansky, K., Silver, T., Mély, D. A., Eldawy, M., Lázaro-Gredilla, M., Lou, X., . . . George, D. (2017). Schema Networks: Zero-shot Transfer with a Generative Causal Model of Intuitive Physics. *Thirty-fourth International Conference on Machine Learning*. Retrieved from <http://proceedings.mlr.press/v70/kansky17a/kansky17a.pdf>
- Knight, W. (2017, September 20). Finally, a Driverless Car with Some Common Sense. *MIT Technology Review*.
- Kovacs, E. (2018, March 08). Cortana Can Expose Enterprises to Attacks, Researchers Warn. *Security Week*. Retrieved from <https://www.securityweek.com/cortana-can-expose-enterprises-attacks-researchers-warn>
- Li, Y., Chang, M.-C., & Lyu, S. (2018). *In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking*. eprint arXiv:1806.02877
- McKinsey & Company. (2017). *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation*. McKinsey & Company.
- Microsoft Corporation. (2018). *Personal Digital Assistant - Cortana Home Assistant - Microsoft*. Retrieved from Microsoft - Official Home Page: <https://www.microsoft.com/en-us/cortana>
- Mnih, V., Kavukcuoglu, K., Silver, D., Graves, A., Antonoglou, I., Wierstra, D., & Riedmiller, M. (2013). *Playing Atari with Deep Reinforcement Learning*. eprint arXiv:1312.5602
- Morgan, S. (2017). *2017 Cybercrime Report*. Cybersecurity Ventures. Retrieved from <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>
- Ng, A. (2016, August 7). IBM's Watson gives proper diagnosis for Japanese leukemia patient after doctors were stumped for months. *New York Daily News*.
- Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 427 - 436). IEEE. 10.1109/CVPR.2015.7298640
- Novikov, I. (2019). Bye-Bye False Positives: Using AI to Improve Detection. BSidesSF.
- Patterson, D. (2018, February 7). *How artificial intelligence is unleashing a new type of cybercrime*. Retrieved from Tech Republic: <https://www.techrepublic.com/article/how-artificial-intelligence-is-unleashing-a-new-type-of-cybercrime/>
- Pinto, L., & Gupta, A. (2015). *Supersizing Self-supervision: Learning to Grasp from 50K Tries and 700 Robot Hours*. eprint arXiv:1509.06825
- Polyakov, A. (2018, February 20). How AI-Driven Systems Can Be Hacked. *Forbes*. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2018/02/20/how-ai-driven-systems-can-be-hacked/#597427979df0>
- Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. (2018). Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police. *Knowledge-Based Systems*, 149, 155–168. doi:10.1016/j.knosys.2018.03.010

- Rodday, N. (2016). Hacking a Professional Drone. RSAConference.
- Rosenfeld, A., Zemel, R., & Tsotsos, J. K. (2018). *The Elephant in the Room*. arXiv:1808.03305 [cs.CV]
- Seymour, J., & Tully, P. (2016). Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter. *Black Hat USA*. Retrieved from <https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf>
- Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., . . . Hassabis, D. (2017). *Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm*. eprint arXiv:1712.01815
- Smith, C. S. (2018, May 10). Alexa and Siri Can Hear This Hidden Command. You Can't. *New York Times*. Retrieved from <https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html>
- Stoecklin, M. P. (2018, August 8). *DeepLocker: How AI Can Power a Stealthy New Breed of Malware*. Retrieved from <https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/>
- Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014). Intriguing properties of neural networks. *International Conference on Learning Representations*.
- Thales eSecurity. (2018). *2018 Thales Data Threat Report*. 451 Research. Retrieved from <http://go.thalesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf>
- The Cylance Team. (2017, August 1). *Black Hat Attendees See AI as Double-Edged Sword*. Retrieved from Threat Vector: https://threatvector.cylance.com/en_us/home/black-hat-attendees-see-ai-as-double-edged-sword.html
- Tilley, A. (2017, February 16). Amazon Alexa Can Now Unlock Your Doors. *Forbes*. Retrieved from <https://www.forbes.com/sites/aarontilley/2017/02/16/amazon-alexa-can-now-unlock-your-front-door/#6c75556875f1>
- Verizon Enterprise. (2018). *Data Breach Investigations Report*. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
- Walker, J. (2017, November 13). AI chatbot used to combat phishing by wasting scammers' time. *Digital Journal*. Retrieved from <http://www.digitaljournal.com/tech-and-science/technology/ai-chatbot-used-to-combat-phishing-by-wasting-scammers-time/article/507506>
- Wallarm. (2018, Nov 19). *Wallarm New Open Source Module and Kaggle Hackathon*. Retrieved from <https://lab.wallarm.com/wallarm-new-open-source-module-and-kaggle-hackathon-8ce0824a967e>
- Walsh, T. (2018). *Machines That Think: The Future of Artificial Intelligence*. Amherst, MA: Prometheus Books.
- Wasserman, T. (2018, March 21). *Chatbots Are All the Rage—and Something of a Risk*. Retrieved from <https://www.securityroundtable.org/chatbots-rage-something-risk/>

Weber, B. (1996, February 18). It's Man Over Machine as Chess Champion Beats Computer He Calls Tough Opponent. *New York Times*.

Webroot. (2017). *Phishing Attacks Growing in Scale and Sophistication*. Retrieved from https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf

Zhou, Y. (2018, May 25). An Oregon family's encounter with Amazon Alexa exposes the privacy problem of smart home devices. *Quartz*. Retrieved from <https://qz.com/1288743/amazon-alexa-echo-spying-on-users-raises-a-data-privacy-problem/>

Crime–Fake News Nexus

Xingyu Chen

 <https://orcid.org/0000-0003-3733-4015>

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

John Yu

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Pamela Goh

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Loo Seng Neo

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Verity Er

Home Team Behavioural Sciences, Ministry of Home Affairs, Singapore

Majeed Khader

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

INTRODUCTION

Following the surge in false stories during the 2016 U.S. elections, there has been increased scrutiny on the phenomenon of fake news by practitioners, academics, and policymakers (Allcott & Gentzkow, 2017; Silverman, 2016). Fake news has gained prominence throughout the world since then, with the intent or potential to undermine public institutions, incite social tensions, and interfere with political processes in affected countries (Select Committee on Deliberate Online Falsehoods, 2018; Tan & Ang, 2017). Consequently, governments worldwide have been deliberating and stepping up on legislative and non-legislative measures to combat the threat of fake news to social and political stability (Hacıyakupoglu, Hui, Suguna, Leong, & Abdul Rahman, 2018). Furthermore, mounting pressure on technology companies to manage the spread of fake news has led tech giants such as Google, Facebook, and Twitter to pioneer efforts to address this problem (Drozdiak, 2018; Foo, 2018).

However, the study and management of fake news is a complex issue. To begin with, the concept of “fake news” is not new as the origins of fake news can be traced back to ancient Rome, where it has been used as a method to consolidate political power. Most famously, during a power struggle for the Roman Empire in 32 BC between Octavian and Mark Anthony, Octavian illegally ‘acquired’ and read out Anthony’s will to the Roman Senate as proof that Mark Anthony had betrayed the Roman people and that he was a puppet of the Egyptian queen Cleopatra (Johnson, 1978). To this date, the degree to which Octavian tampered the contents of the will before he read it out to the Senate, is still debatable (Sirianni, 1984). Nevertheless, history will show that it succeeded in turning the people of Rome against Mark Anthony (MacDonald, 2017). This is just one of many cases where fake news has influenced the way people live their lives.

DOI: 10.4018/978-1-5225-9715-5.ch004

Recognising its potential impact on society and national security, this phenomenon has become an important topic to examine and understand. Existing studies on fake news has focused on different areas of research, such as identifying the actors behind the creation and spread of fake news (Marwick & Lewis, 2017), as well as the psychological vulnerabilities of individuals which contribute to their beliefs in false information (Ecker, Lewandowsky, Fenton, & Martin, 2014).

Another emerging area of concern is the connection between fake news and crime. From the ‘Pizzagate conspiracy’ in the United States which led a man to fire his rifle in a restaurant after conspiracy theorists linked it to a fictitious child sex ring (“‘Pizzagate’ gunman sentenced to four years,” 2017), to false rumours instigating violence and destruction of Muslim properties by Buddhist mobs in Sri Lanka (Taub & Fisher, 2018), fake news has become intertwined with criminal offences of various magnitudes across the globe. Singapore, for example, has also seen a recent emergence of bitcoin investment scams that employ fake news to deceive their victims (Tee, 2018). Despite this emerging nexus between fake news and criminal conduct, there is a dearth of literature examining this convergence to date.

Understanding Crime-Fake News

For the purposes of this chapter, fake news is defined as content that contains inaccurate, misleading, or fabricated information about current events, which is distributed through different channels of communication such as print, broadcast, text messaging, or social media (Chen, Tan, Goh, Ong, & Khader, 2018). Such false content can become implicated with a crime if they are adopted for criminal purposes that result in harm to an individual or society. For example, individuals with malicious intent may spread fake news about a specific group of people being involved in criminal activities in order to incite communal outrage and violence against them (Phartiyal, Patnaik, & Ingram, 2018).

To better examine this association between fake news and crime, the purview of the criminal law needs to be considered. The criminal law, as established and imposed by a state or country, determines which acts constitute a crime and the corresponding punishment associated with them, such as fines or imprisonment, to deter engagement in such acts (Jung, Ahn-Redding, & Allison, 2014). Regarding specific legislation that targets fake news content or people who spread them, only a few countries have implemented and maintained such laws at the time of writing. Under Malaysia’s Anti-Fake News Act, individuals who deliberately spread fake news can be fined or imprisoned, while Germany’s Network Enforcement Act targets the removal of fake news content that is dangerous to public discourse and public peace (Jayakumar, 2018; Venkiteswaran, 2018). Other countries like South Korea and Singapore are mulling over the creation of new laws to combat fake news (Kim, 2018; Sim, 2018).

However, there are existing provisions within the law that can be used to prosecute parties that spread online falsehoods. Within the current Singapore¹ legislative framework, Goh (2018) and Mok (2018) have identified six of such offences that can warrant criminal charges: sending false messages, promoting enmity between races or religions, criminal defamation, sedition, causing public alarm, and spreading fake terrorist threats. Furthermore, there are two more offences of note that are relevant to Singapore. The first is contempt of court which may involve making and spreading false claims that scandalise or undermine the judiciary, while the second concerns unauthorised access to digital data through scams that may employ fake news to lure victims to disclose their personal information (Tee, 2018; “What is the Offence of Contempt of Court?,” 2018). Following the recent recommendation by the Select Committee on Deliberate Online Falsehoods for the Government to “consider supporting or conducting research to understand society’s vulnerabilities” (Select Committee on Deliberate Online Falsehoods, 2018, para. 309) to deliberate online falsehoods, there is a need to widen the evidence base to increase our understanding about this phenomenon.

Thus, an exploratory study on fake news cases (from 2013 to 2018) in Singapore has been conducted. These are crime-fake news cases which have come into contact with the criminal justice system in Singapore. This study also aims to provide an exploratory outlook on the following: (a) the type of crime-fake news in Singapore, (b) the impact that crime-related fake news (or crime-fake news) has on the victims as well as society, (c) the profile of the fake news creators and their motivations, (d) the channels of transmission, as well as (e) the response to mitigate the crime-fake news.

EXPLORATORY STUDY ON FAKE NEWS AND CRIME IN SINGAPORE

Methodology

Data Collection

Online English-language newspaper articles were identified on Google News using the following keywords: ‘Singapore’, ‘false’, ‘misleading’, ‘allegations’, and ‘rumours’, from 1 January 2013 to 1 October 2018. A total of 21,293 online articles were collected.

The start of the data collection was fixed at 2013 as it coincided with the start of the S.U.R.E² campaign. This is Singapore’s first campaign on information literacy awareness, which was launched to improve the general public’s online information literacy and information-seeking habits (Tan, Wan, & Teo, 2014).

32 cases of fake news incidents were subsequently sieved out based on four inclusion criteria. Firstly, in line with the definition of fake news, the case must contain an inaccurate, misleading or fabricated content about current events.

Secondly, it must be an incident that involved Singapore in one of the following ways: (a) an incident that took place in Singapore, (b) an incident where Singapore was directly implicated even if it occurred outside the country, or (c) members of Singapore’s community were involved.

Thirdly, the case must have a criminal element and be serious enough to be implicated with the criminal justice system – whether with the law enforcement agency or the judiciary. As such actions ranging from police reports to court cases are grounds for inclusion.

Lastly, in the event where multiple articles regarding the same fake news incident are present, these articles were counted as a single fake news case.

Coding and Analysis

A content analysis methodology was utilised to analyse the cases. Two independent coders coded the 32 cases along the following domains: type of crime-fake news, impact on Singapore, the identity and motivations of the fake news creator, affected parties, the channel for transmitting fake news, responders to the fake news, and actions taken in response to the fake news. The categories within each domain were developed from a ground-up approach using open, axial, and selective coding (Strauss, 1987). In cases where a consensus on a code could not be achieved, it was resolved via discussions amongst the two coders. For the reliability analysis, Krippendorff’s alpha (α) was run and the values were acceptable (all values where $\alpha > .800$, except for 1 variable where $\alpha = .750$).

ANALYSIS AND DISCUSSION

The Different Types of Crime-Fake News

In order to explore the manifestation of crime-fake news, information on the crime element present in each case was recorded. As a result, seven categories have emerged (see Table 1). The top four most prevalent categories are defamation (e.g., newspaper articles alleging wrongdoing by the local football association), public alarm (e.g., a kidnapping hoax), financial (e.g., a bitcoin investment scam), and false information (e.g., false information which claimed that the local government cancelled *halal* licenses for a large number of eateries).

Table 1 illustrates the three overarching types of crime-fake news. Firstly, there are 6 cases of fake news-assisted crime (18.75%). Within this category, the crime-fake news comprises fraudulent schemes of a financial nature such as get-rich-quick scams (2 cases), phishing scams (3 cases) and one case of an impersonation scam where the scammer impersonated a local politician and began asking for money.

Secondly, there are 8 cases of fake news which harms public order. Fake news under this category are more closely associated with hoaxes (21.88%). This is expected as hoaxes tend to fuel public alarm (e.g., hoaxes inciting fear in parents over stories about child kidnapping in public spaces), which may lead to public unrest amongst those affected by it.

Finally, for fake news-centric crime, there are 18 cases (56.25%). There is a wide range of criminal elements identified amongst the cases, half of which contains defamation (31.25%). This suggests that most crime-fake news incidents are perpetuated to spread false statements online in order to harm the reputation of others.

Table 1. Crime-fake news identified

Crime-fake news	Crime categories	Description	Counts	%
Fake news-centric crime	Defamation	Publishing falsehood intended to defame or harm a person or an entity's reputation.	10	31.25%
	False information	Knowingly spreading false information online that can lead to serious consequences.	4	12.50%
	Contempt of court	Publishing false allegations that scandalises the integrity or impartiality of the judiciary or undermine public confidence in the administration of justice.	2	6.25%
	Sedition	Covers conduct or speech that raises discontent or disaffection among residents of Singapore, brings into hatred or contempt or create dissatisfaction against the government, or promotes ill-will or hostility between different races or classes in Singapore.	2	6.25%
Fake news which harms public order	Public alarm	Knowingly spreading falsehoods that are likely to cause widespread fear and alarm among the public.	7	21.88%
	False terror threat	Spreading false information that causes others to believe that a terrorist act will be carried out.	1	3.13%
Fake news-assisted crime	Financial	Covers fraudulent and dishonest schemes that acquire money, information, or other personal property from unsuspecting individuals.	6	18.75%

The Impact of Crime-Related Fake News on National Security and Social Cohesion

Information regarding the impact of the fake news incident on society was recorded for each incident. As a result, three main categories emerged (see Table 2): (a) fake news which had an impact on national security, (b) fake news which affected social cohesion, and (c) others.

Nine cases (28.13%) had some degree of impact on Singapore's national security. Within this category, it can be further demarcated into three subcategories. For fake news that impacted law enforcement, it revolves around cases which are serious enough to necessitate a response by the authorities. These can be hoaxes which threaten public order (e.g., hoax criminal activities or hoax kidnapping claims), or false accusations about the conduct of law enforcement officers (e.g., a misleading story about a potential police crackdown on a protest). For those associated with terrorism, it refers to terror hoaxes or allegations about an individual being linked to a terror group. Lastly, there are instances where the crime-fake news touch on issues relating to both law enforcement and terrorism.

For social cohesion issues (12.50%), two subcategories were identified: issues affecting race and religion tension (e.g., false claims that Eurasians in Singapore were considered as Indians under Singapore law) as well as xenophobia sentiments (e.g., false claims that foreigners disrupted a religious procession) in Singapore.

Nineteen cases are concerned about other issues (59.38%). These are issues that did not pose a threat to national security and social cohesion. The prevalent subcategories in this category revolved around fraudulent activity (associated with scams), food safety, and contempt of court.

Table 2. Impact in Singapore society

Categories	Subcategories	Counts	%
National Security	Law enforcement	6	18.75%
	Law enforcement + terrorism	2	6.25%
	Terrorism	1	3.13%
Social Cohesion	Xenophobia sentiments	2	6.25%
	Race and Religion issues	2	6.25%
Other Issues	Fraudulent activity	4	12.50%
	Food Safety	3	9.38%
	Contempt of Court	3	9.38%
	Government Actions	2	6.25%
	Environment	2	6.25%
	Defamation	2	6.25%
	Water Contamination	1	3.13%
	Misidentification	1	3.13%
	Deceptive Advertising	1	3.13%

Fake News Creators

Identity of Creators

Several key observations were made during the process of identifying the creators of these crime-fake news. Firstly, in a large proportion of the cases (17 cases; 53.13%), the identities of the fake news creators were difficult to determine due to lack of identifiable information. For example, the identity of the perpetrator could not be established as the perpetrator was using an online alias or that the fake news message was completely anonymous. Secondly, even among those cases where the fake news creators were identified, there were a handful of repeat offenders (which are alternative media outlets in Singapore): The Real Singapore (two cases), The Online Citizen (two cases), All Singapore Stuff (two cases). For the remaining nine cases (28.13%), the identified perpetrator was involved only in one case, and there was no distinct purveyor amongst them.

Motivations

Information on the motivations for the fake news creators was inferred based on (a) the content of the crime-fake news that was transmitted, and (b) if the motivation was reported in the newspaper articles. Table 3 showed the breakdown of the motivations of the fake news creators. Besides a broad range of motivations driving fake news creators, some of them are motivated by more than one motivation. For eight of the cases, there was more than one motivation coded; three motivations coded in two cases, two motivations coded in six cases.

The top four motivations were to influence political outcomes (e.g., claims that a racial minority population was being suppressed by the government), gain profit (e.g., scams), advance social issues (e.g., claiming that the judges were biased against LGBT issues in Singapore), and cause material or reputation harm (e.g., claims that a local business was selling contaminated food with intention to harm the business' reputation). These findings largely corroborated the existing literature on fake news, which identified the endeavour to influence politics and create profit as the main drivers for fake news creators (Chen, 2018; Soon & Goh, 2017; Wardle, 2017). There were also 10 cases in which the motivation was unclear; they were all hoaxes, which are content created by unknown sources with the intent to deceive.

Table 3. Motivations of fake news creators

Categories	Coding description	Counts	%
Politics	Crime-fake news is targeted towards politicians, political parties, or fanning anti-establishment sentiment	11	26.19%
Profit	For the purpose of monetary gain	9	21.43%
Social Issues	To advance an issue that society is concerned about	5	11.90%
Reputational or material harm	Intention has been established to carry out reputational or material harm against an individual or a group	5	11.90%
Seeking Attention/Status	For entertainment value, personal curiosity, personal enjoyment and as a way of gaining status and acceptance within online communities.	1	2.38%
Mistakes	Factual errors made during the process of publication of information for which there has been an apology made or a correction	1	2.38%
Unclear	If the above motivations are not found or no clear indications are present	10	23.81%
Note: more than one motivation may be coded per case as more than one motivation can be present			

Channels of Transmission

Channels of transmitting crime-fake news were inferred by identifying the channel where the message originated from (see Table 4). Crime-fake news had predominantly spread via social media channel (12 cases), with Facebook (8 cases) being the most widely used mode of transmission. This finding is not surprising since Facebook is the most active social media platform in Singapore (We Are Social Singapore, 2017), ensuring that the crime-fake news can achieve a wider outreach.

Another common channel is the local citizen journalism sites (e.g., All Singapore Stuff, STOMP, The Online Citizen etc.), which were seen in 8 cases. One explanation for the prevalence of this category is that these channels would accept and circulate posts from any online contributors. As a result, these posts were often not checked for the veracity of their claims, which makes the channels more susceptible to be exploited by crime-fake news creators.

Response to Mitigate the Crime-Fake News

Information on the actions taken to mitigate the crime-fake news was recorded. In 53.13% of the cases (17 cases), the local authorities were involved in responding to it (see Table 5). Under the category of ‘government’, the Singapore Police Force (6 cases) and the Attorney-General’s Chambers (4 cases) are the most frequent responders to cases of crime-fake news. The Singapore Police Force were mainly responding to cases of public alarm and/or allegations against the police, while the Attorney-General’s Chambers was responding to cases involving contempt of court, the spreading of false information, and sedition.

Concerning the actions taken against the crime-fake news, filing a police report is an action that is commonly employed by affected individuals (77.78%) and private sector/NGO (66.67%). Although there was a sizeable number of private sector/NGO (non-governmental organisation) who responded to fake news, only one of them responded twice (i.e., National Trades Union Congress FairPrice Co-Operative). Nine affected individuals responded to the crime-fake news incident but none of them responded more than once.

Table 4. Channels of transmission

Categories		Counts	(%)
Social Media	(Facebook)	8	24.24%
	(Social Media [Unspecified])	4	12.12%
Citizen journalism sites		8	24.24%
Messaging platform		4	12.12%
Blog		2	6.06%
Website		2	6.06%
Fake website		2	6.06%
Foreign Media		1	3.03%
Offline	(Notes pasted in public spaces)	1	3.03%
Unspecified reports		1	3.03%
Note: more than one channel may be coded per case as more than one channel can be used to spread crime-fake news			

Table 5. Response to fake news in Singapore by responders and action

Responders	Actions taken	Count	(%)
Government	Police statement	7	21.88%
	Police Report	4	12.50%
	Arrest	2	6.25%
	Charged in court	2	6.25%
	Court Order under POHA	2	6.25%
Affected Individual	Police Report	7	21.88%
	Charged in court	2	6.25%
Private Sector/NGO	Police Report	4	12.50%
	Police statement	1	3.13%
	Charged in court	1	3.13%
Notes: An explanation for actions taken categories are as follows: Police Statement: Cases whereby the police issued a formal statement to address the issue due to its potential impact on the public. Police Report: Cases whereby a police report was filed by a victim concerning the false information, warranting further police investigation. Arrest: Cases whereby a police arrest was made due to the offence, but without information on whether the perpetrator was charged in court. Charged in Court: Cases whereby the perpetrator was identified and charged in court for having committed an offence. Court Order (Protection of Harassment Act): Cases whereby a court order addressing the removal of the fake news was issued under the Protection of Harassment Act. In the Singapore legislative framework, Section 15 of the Protection from Harassment Act is a judicial remedy that can be applied to remove statements containing falsehood (Goh, 2018).			

SOLUTIONS AND RECOMMENDATIONS

Accounting for Differences in Fake News Creators

The exploratory study identified seven motivations for creating crime-fake news. As a result, responses against these fake news creators should take into consideration the differences in their motivations, to ensure that appropriate interventions can be identified and implemented. This is important as excessive interventions introduced to mitigate the crime-fake news may create unwanted backlash for the government. This is especially so, when these actions are construed as acts of censorship or state propaganda. In contrast, inaction or inappropriate responses to crime-fake news may inadvertently result in further proliferation of fake news (Pennycook, Cannon, & Rand, 2017).

Engaging with Multiple Stakeholders to Combat Fake News

It might be tempting to think that it is the responsibility of the government to respond to fake news in general, as they have prior experience in responding to such incidents, and that they have more resources at their disposal to do so. However, given the accelerated rate at which information is created and disseminated online, it is not feasible for the authorities to monitor and respond to all incidents of crime-fake news. Therefore, there is a need for authorities to engage with multiple stakeholders to combat crime-fake news.

Working With Social Media Companies to Curb the Spread of Fake News

As seen in Table 4, the most prevalent channel for transmitting crime-fake news is through Facebook, which highlights the need for social media companies to be involved in combating fake news. While social media companies are not direct creators of fake news, the abuse of their platforms and online services to propagate fake news places a responsibility on these companies to play a role in keeping the global information ecosystem safe from malevolent actors. As the Select Committee on Deliberate Online Falsehoods noted, “Technology companies have a social responsibility to contribute to a clean Internet information ecosystem” (Select Committee on Deliberate Online Falsehoods, 2018, para. 463).

Authorities can work with social media companies to develop reporting resources to enable the online community to self-police the platforms where the spread of crime-fake news occurs. From a crime prevention perspective, the development of such resources can increase the operating risk of spreading crime-fake news on these platforms for potential offenders (Holt & Bossler, 2016), as the online community is empowered to report those who peddle fake news with criminal intent.

Additionally, social media companies are best placed to combat fake news as they have the capabilities to take down, monitor, and detect the spread of fake news on their platforms (Weedon, Nuland, & Stamos, 2017). Thus, these companies can work in tandem with law enforcement to shut down crime-fake news and take action against the offenders.

Building a Media-Literate Citizenry

It is important to build a media-literate citizenry who can exercise scepticism and critical thinking as they consume information online. In Singapore, the National Library Board of Singapore launched a S.U.R.E campaign to increase information literacy in the public by encouraging individuals to perform four steps when handling information: (1) check whether the information source is reliable, (2) understand the context of the information, (3) research into other sources to verify the accuracy of information (cross-check), (4) evaluate the best way to use the information (Tan et al., 2014). In addition, skills such as fact-checking and understanding the effect of cognitive biases (Soon & Goh, 2017) can prepare the public to combat fake news in general.

Another avenue to enhance media literacy and deter potential perpetrators is to inform users on what behaviours are acceptable and unacceptable in online communities. This ensures that they apprehend the implications and consequences of creating and spreading fake news online. Such measures can be implemented through ‘Internet Use Policies’ that informs users of the rules that they have to abide by, such as the prohibition of inflammatory or discriminatory statements (Holt & Bossler, 2016). If any user ends up posting and spreading fake news within these sites despite agreeing to them, then they would not be able to use the excuse that they did so out of ignorance or without ill-intent.

FUTURE DIRECTIONS

This current study is an exploratory research on the emergence of a crime-fake news nexus in Singapore. It is important to recognise the limitations associated with the study. For example, it is possible that certain crime-fake news incidents were missed because it was not prominent enough, and/or that the fake

news was reported through non-English language articles (which were not picked up during the search process). Thus, future research should examine crime-fake news that are propagated in other languages such as Mandarin, Malay, or Tamil. This may widen the evidence base for informing the creation and implementation of policies to contain the spread of crime-fake news.

CONCLUSION

Fake news can exert a profound impact on society, especially when they are also associated with criminal activities. The present exploratory study into the nexus between fake news and crime paints a complex picture of this phenomenon. It attempts to highlight the various types of crime-fake news, the impact it can have on the society, the different motivations driving each case, the channels used to transmit fake news, and the different responses taken to mitigate each fake news case. By identifying contours in this nexus of fake news and crime, this study hopes to contribute to and guide future research in this area.

REFERENCES

- Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *The Journal of Economic Perspectives*, 31(2), 211–236. doi:10.1257/jep.31.2.211
- Chen, X., Tan, J., Goh, P., Ong, G., & Khader, M. (2018). *Frequently Asked Questions about Fake News* [HTBSC Research Report S02/2018]. Singapore: Home Team Behavioural Sciences Centre.
- Chen, X. K. (2018). Fake News After a Terror Attack: Psychological Vulnerabilities Exploited by Fake News Creators. In M. Khader, L. S. Neo, D. D. Cheong, & J. Chin (Eds.), *Learning from Violent Extremist Attacks: Behavioural Sciences Insights for practitioners and policymakers* (pp. 435–451). World Scientific Press. doi:10.1142/9789813275447_0023
- Drozdiak, N. (2018, September 26). Google, Facebook and Twitter Agree to Fight Fake News in the EU. *Bloomberg*. Retrieved from <https://www.bloomberg.com/news/articles/2018-09-25/google-facebook-and-twitter-agree-to-fight-fake-news-in-eu>
- Ecker, U. K., Lewandowsky, S., Fenton, O., & Martin, K. (2014). Do people keep believing because they want to? Preexisting attitudes and the continued influence of misinformation. *Memory & Cognition*, 42(2), 292–304. doi:10.375813421-013-0358-x PMID:24005789
- Foo, Y. C. (2018, September 26). Facebook, Google to tackle spread of fake news, advisors want more. *Reuters*. Retrieved from <https://www.reuters.com/article/us-eu-tech-fakenews/facebook-google-agree-to-tackle-fake-news-eu-idUSKCN1M61AG>
- Goh, Y. (2018). *Written Representations to the Select Committee on Deliberate Online Falsehoods; Effectiveness of Current Legislative Tools (Paper No. 129)*. Retrieved from Parliament of Singapore website: <https://www.parliament.gov.sg/docs/default-source/sconlinefalsehoods/written-representation-129.pdf>

Haciyakupoglu, G., Hui, J. Y., Suguna, V., Leong, D., & Abdul Rahman, M. F. (2018). *Countering Fake News: A Survey of Recent Global Initiatives*. Retrieved from S. Rajaratnam School of International Studies website: <http://hdl.handle.net/11540/8063>

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. New York: Routledge.

Jayakumar, S. (2018). *Germany's NetzDG: Template for Dealing with Fake News?* S. Rajaratnam School of International Studies.

Johnson, J. R. (1978). The Authenticity and Validity of Antony's will. *L'Antiquite Classique*, 47(2), 494–503. doi:10.3406/antiqu.1978.1908

Jung, S., Ahn-Redding, H., & Allison, M. (2014). Crimes and punishment: Understanding of the criminal code. *Canadian Journal of Criminology and Criminal Justice*, 56(3), 341–366. doi:10.3138/cjccj.2013.E17

Kim, T. H. (2018, October 26). South Korean war on “fake news” raises concern of censorship. *Associated Press*. Retrieved from <https://www.apnews.com/3d14a9663b114644a36e123a7c7bf9b1>

MacDonald, E. (2017, January 13). The fake news that sealed the fate of Antony and Cleopatra. *The Conversation*. Retrieved from <http://theconversation.com/the-fake-news-that-sealed-the-fate-of-antony-and-cleopatra-71287>

Marwick, A., & Lewis, R. (2017). *Media manipulation and disinformation online*. Data & Society.

Mok, Z. C. (2018, March 28). *Spreading Fake News in Singapore Could Get You Punished with These 6 Crimes*. Retrieved from SingaporeLegalAdvice.com website: <https://singaporelegaladvice.com/spreading-fake-news-singapore-crimes>

Pennycook, G., Cannon, T. D., & Rand, D. G. (2017). Prior exposure increases perceived accuracy of fake news. *SSRN*. Retrieved from <https://ssrn.com/abstract=2958246>

Phartiyal, S., Patnaik, S., & Ingram, D. (2018, June 25). When a text can trigger a lynching: WhatsApp struggles with incendiary messages in India. *Reuters*. Retrieved from <https://www.reuters.com/article/us-facebook-india-whatsapp-fake-news-idUSKBN1JL0OW>

“Pizzagate” gunman sentenced to four years. (2017, June 22). *BBC News*. Retrieved from <https://www.bbc.com/news/world-us-canada-40372407>

Select Committee on Deliberate Online Falsehoods. (2018). *Report Of The Select Committee On Deliberate Online Falsehoods – Causes*. Singapore: Consequences And Countermeasures.

Silverman, C. (2016, November 17). This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. *BuzzFeed*. Retrieved from <https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>

Sim, R. (2018, September 20). Select Committee on fake news: 22 recommendations unveiled to combat online falsehoods. *The Straits Times*. Retrieved from <https://www.straitstimes.com/singapore/select-committee-on-fake-news-22-recommendations-unveiled-to-combat-online-falsehoods>

Sirianni, F. A. (1984). Was Antony's Will partially forged? *L'Antiquite Classique*, 53(1), 236–241. doi:10.3406/antiqu.1984.2126

Soon, C. W. T., & Goh, Z. S. S. (2017). *What Lies Beneath the Truth: A Literature Review on Fake News, False Information and More*. Institute of Policy Studies.

Strauss, A. L. (1987). Codes and Coding. In *Qualitative analysis for social scientists* (pp. 55–81). Cambridge University Press. doi:10.1017/CBO9780511557842.004

Tan, E. E. G., & Ang, B. (2017). *Clickbait: Fake News and Role of the State*. RSIS.

Tan, G., Wan, W. P., & Teo, J. (2014). *SURE Campaign: Promoting Information Literacy Awareness to Singaporeans*. Presented at the IFLA WLIC 2014 - Lyon - Libraries, Citizens, Societies: Confluence for Knowledge.

Taub, A., & Fisher, M. (2018, April 21). Where Countries Are Tinderboxes and Facebook Is a Match - The New York Times. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/04/21/world/asia/facebook-sri-lanka-riots.html>

Tee, Z. (2018, September 19). Bitcoin scam online using fake comments attributed to Tharman: MAS. *The Straits Times*. Retrieved from <https://www.straitstimes.com/business/bitcoin-scam-online-using-fake-comments-by-tharman-mas>

Venkiteswaran, G. (2018, September 23). Fake news still a crime in Malaysia. *The Star Online*. Retrieved from <https://www.thestar.com.my/news/nation/2018/09/23/fake-news-still-a-crime-in-malaysia-in-this-transition-period-where-rules-are-constantly-being-negot/>

Wardle, C. (2017, February 16). *Fake news. It's complicated*. Retrieved January 23, 2018, from First Draft News website: <https://firstdraftnews.com:443/fake-news-complicated/>

We Are Social Singapore. (2017, January). *Digital in 2017: Southeast Asia*. Internet. Retrieved from <https://www.slideshare.net/wearesocialsg/digital-in-2017-southeast-asia>

Weedon, J., Nuland, W., & Stamos, A. (2017). *Information Operations and Facebook*. Facebook Security.

What is the Offence of Contempt of Court in Singapore? (2018, November 2). Retrieved from SingaporeLegalAdvice.com website: <https://singaporelegaladvice.com/law-articles/contempt-of-court-singapore>

ADDITIONAL READING

Caspi, A., & Gorsky, P. (2006). Online deception: Prevalence, motivation, and emotion. *Cyberpsychology & Behavior*, 9(1), 54–59.

Chen, X. (2018). Fake News After a Terror Attack: Psychological Vulnerabilities Exploited by Fake News Creators. In M. Khader, L. S. Neo, D. D. Cheong, & J. Chin (Eds.), *Learning from Violent Extremist Attacks: Behavioural Sciences Insights for practitioners and policymakers* (pp. 435–451). World Scientific Press.

Cook, J., & Lewandowsky, S. (2011). *The Debunking Handbook*. St. Lucia, Australia: University of Queensland.

Ecker, U. K., Lewandowsky, S., Chang, E. P., & Pillai, R. (2014). The effects of subtle misinformation in news headlines. *Journal of Experimental Psychology. Applied*, 20(4), 323.

Jack, C. (2017). *Lexicon of Lies: Terms for Problematic Information* (Media Manipulation). Data & Society Research Institute.

Neubronner, S. (2017). *Social Media and “Fake News”: Impact on Social Cohesion in Singapore (RSIS Commentaries)*. Singapore: Nanyang Technological University.

Silverman, C. (2016, November 17). This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. *BuzzFeed*. Retrieved from <https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>

Tandoc, E. C. Jr, Lim, Z. W., & Ling, R. (2018). Defining “fake news” A typology of scholarly definitions. *Digital Journalism*, 6(2), 137–153.

Whitty, M. T., & Young, G. (2016). *Cyberpsychology: The study of individuals, society and digital technologies*. Wiley.

KEY TERMS AND DEFINITIONS

Alternative Media Outlets: In Singapore, this refers to platforms which are not under the ownership of Singapore’s mainstream media organisations: Mediacorp and Singapore Press Holdings. These sites predominantly accept posts from contributors who may be anonymous.

Axial Coding: The process of identifying the relationships between the categories and linking them together. The process yields subcategories that are grouped under a specific category. This process takes place after open coding.

Crime-Fake News: Fake news content which commits a transgression within the legal system in Singapore that can warrant a fine, imprisonment, or both.

Fake News: Content that contains inaccurate, misleading, or fabricated information about current events, which is being distributed through different channels of communication such as print, broadcast, text messaging, or social media.

Open Coding: The process of repeating readings of media sources and a line-by-line analysis of the data in order to open up the data to understand the meanings and concepts in it. Open coding includes the labelling of concepts and creating categories for comparison.

Select Committee on Deliberate Online Falsehoods: In 2018, a Select Committee on Deliberate Online Falsehoods was set up by Singapore’s parliament to examine and report on the phenomenon of the use of digital technology to spread falsehoods online. They have since unveiled 22 recommendations to combat online falsehoods.

Selective Coding: The process of further linking the categories from axial coding into a core category. This process takes place after axial coding.

ENDNOTES

- ¹ The discussion on the laws are presented here only for discussion purposes. As there are always amendments to the law over the years and new Bills being passed in Parliament. Information is up to date as of Dec 2018. This is because Singapore passed a law in April concerning fake news, which means that information is not updated at this stage.
- ² The National Library Board branded the information literacy campaign as S.U.R.E., which stands for Source, Understand, Research and Evaluate. It encourages people to do 4 steps when handling information: (1) check whether the information source is reliable, (2) understand the context of the information, (3) research into other sources to verify the accuracy of information (cross-check), (4) evaluate the best way to use the information.

Unveiling Cybercrime in a Developing Country

Richard Boateng

 <https://orcid.org/0000-0002-9995-3340>

University of Ghana Business School, Ghana

Jonathan Nii Barnor Barnor

University of Ghana Business School, Ghana

INTRODUCTION

Information and communication technology (ICT) networks, devices and services are increasingly critical for day-to-day activities (ITU, 2015). These ICTs arguably have therefore become necessary elements in our everyday lives and businesses for the past few decades (Bankole & Bankole, 2017). Despite the enormous benefits of ICTs, there exist a myriad of malicious use of these technologies which translate into financial loss to individuals, organizations and States. Unmistakably, cybercrime poses the biggest threat to the digital society (van de Weijer & Leukfeldt, 2017). Whereas the cost of cybercrime in 2015 was valued at \$3 trillion (Cybersecurity Ventures, 2017), Forbes (2017) conjecture that that figure will double to approximately \$6 trillion per year on average through 2021.

Extant literature have discussed cybercrime in various perspectives, for example, its impact (Ananthakrishnan, Li, & Smith, 2015; Riek, Abramova, & Böhme, 2017), detection and defensive measures in the fight against cybercrime (Biswas, Pal, & Mukhopadhyay, 2016; Tapanainen, 2017; Zhang, Lee, & Wang, 2016), law enforcement, strategies and prevention (Alanezi & Brooks, 2014; Ju, Cho, Lee, & Ahn, 2016; Kolini & Janczewski, 2017). Even though these studies are only a few of what exists in the respective themes, a preliminary review indicated that very few of these studies had been done with particular focus on the socioeconomic drivers behind the commission of cyber offences especially in developing economies.

According to the ITU (2012) The term “cybercrime” is used to describe a range of offences including traditional computer crimes, as well as network crimes. As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue, while excluding traditional crimes that are just facilitated by using hardware. Such crimes may include hacking, bullying, identity theft, confidence romance, advanced fee fraud, among others. Riek and Böhme (2018) for instance posited that losses as a result of cybercrime are driven mainly by scams and extortion in Germany and identity thefts in the UK. Italian, Estonian, and Polish consumers on the other end, lose considerably less money to cyber-criminals, even though they spend less money and time on protection. Whereas this development is relative to the western countries, the situation is not entirely different in Africa. Cross (2018) for instance asserts that Nigeria has become synonymous with online fraud, with advance fee fraud (AFF) dominating in recent decades.

DOI: 10.4018/978-1-5225-9715-5.ch005

Consequently, Nigeria ranked as the leading State in the region for the conducting of malicious Internet activities (Aransiola & Asindemade, 2011; Longe & Chiemeke, 2008; Quarshie & Martin-Odoom, 2012). That notwithstanding, many countries in the continent have developed legislation to fight cyber-threats. They have also strengthened enforcement measure as well as engage private sector efforts to enhance cybersecurity (Kshetri, 2017). In East Africa for example, a task force comprising government, industry and civic groups have been set up to deal with cybersecurity at the three levels of legal, policy, and regulation. While the Economic Community of West African States (ECOWAS) have initiated policies in capacity-building, prioritising cybercrime issues and developing networks across the borders as a definite way in fighting cybercrime (Quarshie & Martin-Odoom, 2012).

Ghana, our country of focus formulated two policies; ICT for Accelerated Development Policy of 2003 and the National Telecommunications Policy of 2005 both aimed at facilitating the country's development into an information society. The sub-Saharan country also has a vision of developing its economy to a middle-income level, and thus requires the development and exploitation of ICT both as a business sector and as an enabler of other sectors (Frempong, 2012). Further, Internet penetration in the country for the past few years has been on the ascendancy. Hootsuite (2018) for instance reports that about 10.11 million representing 35% of the population are active internet users with 32% active phone internet users. With this statistics in perspective, it will arguably not be out of place to contend that as more and more people get access to data, we expect cases of cybercrime to escalate (National Communications Authority, 2017). With this backbone, this chapter seeks to answer these research questions. First, what are the motivating factors to the commission of internet crimes in developing countries and second, what are the perceptions of stakeholders in the fight against cybercrime?

This paper is in eight sections with the first giving a broad overview of cybercrime by way of introduction, review of cybercrime literature and the theoretical foundation of cybercrime. The fourth and fifth sections explain the methodology of the research and further presents the findings of cybercrime in Ghana. The final two sections include the conclusion and the summary of the findings indicating implications for research, practice and policy and pointers for future research.

LITERATURE REVIEW

There exists a significant volume of research on cybercrime and its attendant effects on countries and the social stigmatization that accompanies them. These literature cover a number of relevant themes which include but not limited to the fight against cybercrime (Cassim, 2011; Adomi & Igun, 2008; Malgwi, 2005; Jamil, 2012; Huey, Nhan & Broll, 2012), credit card fraud or financial crimes (Barker, D'Amato & Sheridan, 2008; Gottschalk, 2010; Prabowo, 2012), Advance fee fraud (Durkin & Brinkman, 2009; Dobovsek, Lamberger & Slak, 2013; Salu, 2005), Law enforcement (Davis, 2012) and Confident Romance and dating (Fair, Tully, Ekdale & Asante, 2009).

Onwuegbuzie, Leech and Collins (2013) postulate that a thorough, sophisticated literature review is the foundation and inspiration for substantial, useful research. It is therefore helpful in two ways; thus, it does not only help researchers glean the ideas of others interested in a particular research question, but it also lets them read about the results of other (similar or related) studies. The definition of the spectrum of cybercrime has also been an issue of contention especially considering the dynamics of the phenomenon (see Table 1) (ITU, 2012). Adomi and Igun (2008) defined cybercrime as *any unlawful conduct carried out with the use of computers, electronic and ancillary devices*. Cassim (2011) also contends that

Table 1. Definitions and factors considered

Author (s)	Definition/characteristics of cybercrime	Internet fraud	Computer hacking	Cyber piracy	Spreading of malicious code	Others
Cassim (2011)	On one hand, a computer may become the 'object' of a crime when a computer hardware or software occurs. On the other hand, a computer becomes the 'subject' of a crime when it is used as an 'instrument' to commit traditional crimes.	✓	✓	✓	✓	✓
(Adomi & Igun (2008)	Any unlawful conduct carried out with the use of computers, electronic and ancillary devices	✓	✓		✓	✓
Loader & Thomas (2013)	Computer-mediated activities which are either illegal or considered illicit by certain parties which can be conducted through global electronic networks.	✓	✓	✓	✓	✓
Chung, Chen, Chang, & Chou (2006)	Illegal computer-mediated activities that often take place in the global electronic networks.	✓	✓	✓	✓	✓
Longe et al., (2009)	Cybercrime refer to misconducts in the cyber space as well as wrongful use of the internet for criminal purposes	✓			✓	✓
Gordon & Ford (2006)	Any crime that is facilitated or committed using a computer, network, or hardware device	✓*	✓		✓	✓
Kshetri (2009)	Criminal activities in which computers or computer networks are the principal means of committing an offense	✓	✓			✓
ITU (2012)	a range of offences including traditional computer crimes, as well as network crimes.	✓	✓	✓	✓	✓

Cybercrime, also known as 'computer crime' appears to have no precise definition. On one hand, a computer may become the 'object' of a crime when a computer hardware or software occurs. On the other hand, a computer becomes the 'subject' of a crime when it is used as an 'instrument' to commit traditional crimes such as fraud, theft, extortion, 'new' types of activities such as denial of service attacks and malware, identity theft, pornography, or copyright infringement.

For the purpose of this research, this chapter will define cybercrime as *any unlawful conduct executed with the aid of any computing device or other forms of ICTs*. This includes but not limited to advance fee fraud, cyber harassment, illegal online shopping, Credit Card Fraud, Confidence Fraud/Romance, child pornography et cetera.

It must however be well noted that in as much as developing countries are touting the potential of the internet for national development, they are also cautious of the potential dangers posed by its misuse. The negative impacts of cyber fraud are both economic and social (Durkin & Brinkman, 2009). Further, from the perspective of ICT for development, it is not misplaced to say that cybercrime portends some dangers and have the potential to stall the developmental contributions accruable from a well-harnessed ICT adoption, diffusion and usage in Sub-Saharan Africa (Boateng, Olumide, Isabalija, & Budu, 2011).

Several studies have been done with the Sub-Saharan region in focus. These studies follow quite a wide range of themes (some of such have been indicated in Table 2). Inasmuch as these studies are exhaustive, there is a lack of concentration on the roles IT skills play in the commission of a crime. Aransiola and Asindemade (2011) in studying new strategies employed by cybercriminals in Nigeria identified imperceptible aids including the use of ladies as collaborators, collaboration with security agents and bank officials, local and international networking, and the use of voodoo. A similar study by Warner (2011) sought to give account on the broad overview of Ghanaian cybercrime, focusing on its genesis, the various incarnations of national scams and the state-level reactions. The study claimed that most Ghanaian believe cybercrime was imported from Nigeria as a result of the influx of Nigeria Nationals residing in Ghana; geopolitics. Secondly, Warner (2011) similarly to Tade, (2013) identified that the delayed success rates in *yahoo yahoo*, the untiring clampdown of the Economic and Financial Crimes Commission on cybercriminals, group rivalry and the activities of the media in enlightening the public accounted for the search for a more speedy way of increasing cybercrime victimisation hence the *techno-spiritual paradigm of Sakawa*. Finally, Warner (2011) identified that perpetrators of cybercrime in Ghana justified their actions with the assertion that there is nothing wrong with the act but a sort of redemptive project of social justice; vengeance for centuries of historical injustices perpetrated by the West against Africans. Again, even though the findings by Warner (2011) gives grounds to further studies in cybercrime especially in Ghana, the study dwelt on secondary data; the data collected did not include perpetrators of cybercrime but the views of individuals on cybercrime in Ghana.

Despite the enormous contributions of these studies, there seem to be a gap in the understanding of cybercrime from the viewpoint of cybercrime perpetrators *vis a vis* law enforcement agencies and secondary stakeholders. Further, theories employed in studying computer related crimes remain sparse considering the dynamic nature of the phenomenon. Boateng, Olumide, Isabalija and Budu (2011) underscored the need for future studies to explore how social theories in criminal studies can help in understanding behaviour and intention of both the victims and perpetrators in cybercrime. This chapter provides useful insights in response to these gaps.

THEORETICAL FOUNDATION

A number of criminological and social theories have been postulated to explain criminal activities and the behaviour of conventional criminals. However, empirical research to validate these theories in the context of cyber activities and the application of these theories to cybercrime are sparse in literature (Wada, Longe, & Danquah, 2012). These include but not limited to Routine Activity Theory (Cox, Johnson, & Richards, 2009; Jansen & Leukfeldt, 2015; Olayemi, 2014; Reyns, 2013), Space transition theory (Danquah & Longe, 2011; Jaishankar, 2008), Protection motivation theory (Jansen & Leukfeldt, 2015). Inasmuch as these theories are relevant to cybercrime studies, there have also been calls for future studies to explore how social theories in criminology can assist in understanding the behaviour and intention of both the victim and perpetrators in cybercrime (Boateng et al., 2011; Holt & Bossler, 2014; Jaishankar, 2008).

Table 2. Cybercrime studies in Ghana and Nigeria

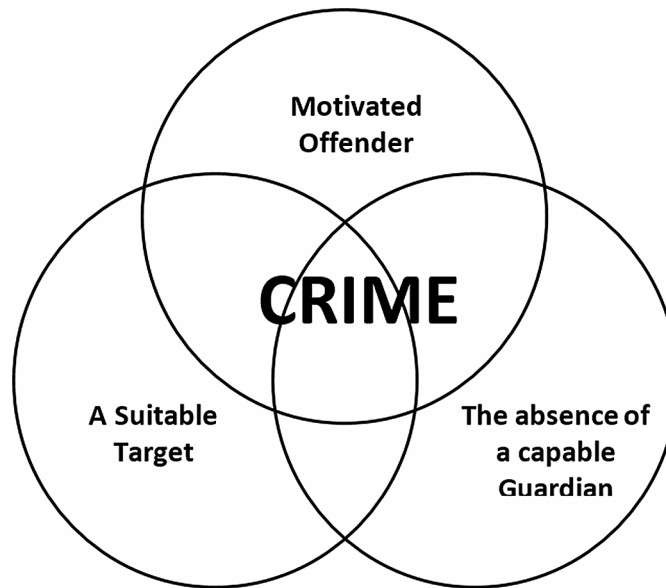
Article	Country and Perspective	Theme / Theory	Findings
Tade (2013)	Nigeria Student [Cybercrime] fraudsters	Cybercrime and spirituality Theory: <i>Space transition theory</i>	The delayed success rates in yahoo yahoo, the untiring clampdown of the Economic and Financial Crimes Commission on cybercriminals, group rivalry and the activities of the media in enlightening the public accounted for the search for a more speedy way of increasing cybercrime victimisation.
Quarshie & Martin-Odoom (2012)	East and West Africa Content Analysis	Legal and regulatory frameworks Theory: <i>Not Considered</i>	The research revealed that the way forward is for Africa to learn from the experience of developed countries in fighting cybercrime. The fight against cybercrime requires a coordinated effort among all stakeholders such as government bodies, educational institutions, business organizations and law enforcement authorities.
Olayemi (2014)	Nigeria Law Enforcement Agencies, Governmental Institution	Legal and regulatory frameworks Theories: <i>Routine Activity Theory</i> <i>Structural Functionalism Theory</i> <i>Marxian Theory</i> <i>The Theory of Technology-Enabled Crime</i>	Laws to combat cybercrimes are useless if law enforcement agencies do not have the education and training necessary even to operate a computer. Judges must be well trained as well
Aransiola & Asindemade (2011)	Nigeria Perpetrators	New cybercrime strategies Theory: <i>Not Considered</i>	Most cybercrime perpetrators in Nigeria are between the age of 22 and 29 years who were undergraduates and have distinctive lifestyles from other youths. Their strategies include collaboration with security agents and bank officials, local and international networking, and the use of voodoo, thus traditional supernatural power. Findings also indicated that most perpetrators of cybercrime were involved in online dating and buying and selling with fake identity among others.
Warner (2011)	Ghana Perpetrators*	Geopolitics Techno-spiritual paradigm (Sakawa) Justified Philosophy of Thievery Theory: <i>Not Considered</i>	Sakawa boys justify their duping of Westerners by claiming that it is pointed retribution for centuries of historical injustices perpetrated by the West against Africans. The rise and proliferation of the techno-religious phenomenon of Sakawa is another increasingly embedded, yet underreported aspect of the practice of Internet fraudulence in Ghana.
Boateng, Olumide, Isabalija, & Budu (2011)	Ghana Internet Café Operators Law Enforcement agencies Lawyers Banks	Forms and implications of cybercrime Theory: <i>Not Considered</i>	Cybercrime is fast gaining grounds in Ghana and the agencies responsible for investigating, controlling and apprehending online criminals lack the technical knowledge needed to tackle the problem. In Ghana, the perpetrators are young and have some degree of technical competence to commit computer-related crimes.

Source: Literature synthesis

The Routine Activity Theory

The Routine Activity Theory (RAT) postulated by Cohen and Felson (1979) is an ecological approach to crime causation, and the accessibility, location, and presence or absence of environmental characteristics, and certain types of people are what proves predictive of criminal behaviour. It presupposes that for a crime to take effect, three required elements must be present. First is the motivated offender, second, a suitable target; The suitable target here refers to a person, object or place and finally, the absence of capable guardians; a deterrent like police patrols, security guards, neighbourhood watch, door staff, vigilant staff and co-workers, friends, neighbours and CCTV systems (Wada et al., 2012) (see Figure 1).

Figure 1. The routine activity theory of crime



The RAT even though was originally postulated as a traditional crime theory has been adapted and used in various cybercrime studies (e.g. Cox, Johnson, & Richards, 2009; Reyns, 2013; Xiao, Chan, Cheung, & Wong, 2016; Yar, 2005) because of its robustness. Table 3 illustrates the various forms of cyber offences the theory has been used to study as well as the consideration as sole or combined theory.

Despite these advancements in literature, focus on the technological aspect of the RAT is sparse as most scholars employ the use of the theory as is, or combine it with other theories to answer peculiar questions. This therefore perhaps prompted some researchers (Eck & Clarke, 2003; Holtfreter, Reisig, & Pratt, 2008; Pratt et al., 2010) to explore the possibilities of using the theory to explain opportunities for crimes at a distance (Reyns, 2013). Eck and Clarke (2003) for instance argued that the traditional Routine Activity Theory proposed by Cohen and Felson (1979) *could be expanded by making one modification*.

Table 3. Routine activity theory in cybercrime studies

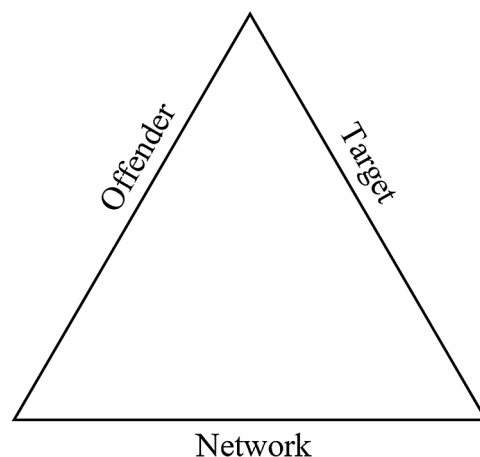
Studies	Forms of cybercrime	Usage	Other theories
Olayemi (2014)	General	Combined	• Structural Functionalism Theory • Marxian Theory • The Theory of Technology-Enabled Crime
Kigerl (2012)	General	Sole	N/A
Reyns (2013)	Identity Theft	Sole	N/A
Reyns, Henson, & Fisher (2011)	Cyberstalking	Sole	N/A
Navarro & Jasinski, (2012)	Cyberbullying	Sole	N/A
Pratt, Holtfreter, & Reisig (2010)	Fraud	Sole	N/A
Leukfeldt (2014)	Phishing	Sole	N/A
Reyns & Henson (2016)	Identity Theft	Sole	N/A

Source: Literature synthesis

In their view, if the target and the offender are part of the same geographically dispersed network, then the offender may be able to reach the target through the network. Eck and Clarke (2003) further posit that networks do not only facilitate interaction at a distance; they can also increase the speed of distant contacts. For instance, whereas traditional crime under the routine activity theory may unfold slowly and may occur over a long period, the internet can increase the speed with which the same sorts of frauds can unfold. Tillyer and Eck (2009) advanced this argument by establishing that the RAT focusses on offenders making contact with targets at physical locations, which therefore creates a void in studying crimes that occur at a distance. Tillyer and Eck (2009) finally suggested that either the routine activities theory is limited to place-based crimes or it needs revision.

These developments have arguably made it imperative to conceptualise the RAT in terms of current trends in technologies and technology related crimes. For instance, the three elements of the RAT may exist; the motivated offender, the target and the absence of a deterring factor but in the midst of all these, what role does knowledge in technology play in the triad? This further translates into investigating the interrelationship between technology and the constructs of the RAT. Eck & Clarke (2003) in critiquing the theory suggested the inclusion of networks as represented in Figure 2. However, this chapter conceptualises the theory with the integration of Eck and Clarke (2003) network to the original theory; motivated offender, suitable target, absence of a capable guardian and Network. To this end, the study will first unveil the categories of people who fall under the offender's construct. Secondly, concerning the victims of cyber offences as postulated by the theory, the chapter will solicit the categories of victims that the offenders target and their characteristics. This will enable the researchers to understand the victims from the perspective of the offenders. The third is to understand the role of guardianship in forestalling cyber offences. This will be done by engaging law enforcement agents and law practitioners. Finally, with respect to technology and networks which form the basis of our arguments, the chapter will seek to bring to bear the facilitating roles played by emerging technologies and the commission and prevention of internet crimes.

Figure 2. Systems problems



METHODOLOGY

1

This section presents the methodology adopted for this chapter. It covers the research paradigm employed as well as strategies for data collection and the mode of analysis. In order to achieve the research purpose of this chapter, the critical realist stance was adopted. Critical realism enables the researcher to unearth the mechanisms that cause events to occur (Mingers, 2004). This lays a strong foundation for this study, in that it goes beyond the generalization of all IT related crimes as cybercrime, to a detailed exposition of the social and economic motivations of the offender as well as the technological aids. With this in perspective, there is therefore the need to understand how CR can be employed in conducting such a study.

To address this, this chapter adopted a retroduction research strategy which is peculiar to the critical realists (Scott, Zachariadis, & Barrett, 2013; Strong & Volkoff, 2010). Retroduction allows researchers to move between the knowledge of empirical phenomena as expressed through events to the creation of explanations (or hypothesizing) in ways that hold “ontological depth” and can potentially give some indications on the existence of unobservable entities (Downward & Mearman, 2006). Retroduction according to (Danermark, Ekström, Jakobsen, & Karlsson, 1997) poses one fundamental question. In this case, *what properties must exist for cybercrime to exist and to what extent is cybercrime?* The dexterity of retroduction lies in its ability to aid a researcher to establish generative mechanisms for phenomena such as cybercrime to exist. Taking this as one’s starting point, retroduction becomes a matter of trying to attain knowledge about what internal relations make cybercrime what it is (Danermark et al., 1997).

Three main phases manifest in employing the retroductive research strategy for a study. At the initial stage, the authors began by examining the observed events and connections in the social phenomena. At this level, the researcher is required to conduct a thorough literature review on cybercrime to bring to bear the theoretical and conceptual underpinnings which have been used to explain cybercrime in previous studies (see section 1.2). Next, the authors hypothesized the presence of real structures and mechanism and how they describe the observed relationships. In the critical realist’s viewpoint, this is done through theorising a model of an underlying mechanism which might have produced patterns seen in the data and then works backwards from the data towards verifying or otherwise that model (Mason, 2002). This step has been well outlined in 1.3 of this chapter by first adopting the routine activity theory of crime and thence conceptualising it to include networks as pointed out by Eck and Clarke (2003). Finally, the third step is to establish that the structures and mechanisms postulated in section 1.2 operate and exist. The researcher then needs to select suitable data collection methods that support the purpose of the study.

Case Selections

For the purpose of studying contemporary socio-technical phenomenon to uncover the causal mechanisms and contextual factors that combined to generate them, case study research is well-suited to conduct critical realist research (Wynn & Williams, 2012). Boateng (2014) suggests that case selection requires the researcher to be knowledgeable about the characteristics of the case before the beginning of the main case study. With this in mind, a pilot study was conducted in March 2017 and the main study between August and September 2018. Due to privacy and the nature of the study, some respondents during the pilot study opted to hold interviews via phone conversation rather than a face to face interaction. The rest of the interviews were then scheduled at the internet café where the respondents occasionally operate. After the pilot study, four out of a total of seven respondents agreed to participate in the study. The

four were a group of young men who operate together from the same room (which they refer to as ‘the office’). A plausible reason for the other three’s refusal to participate could be that one of them is in the process of withdrawing from the act and in undergoing personal rehabilitation. The other two’s refusal was on the grounds of privacy. The selection of one case for this research stems from the fact that unlike positivist research which seeks statistical significance, a CR-based case study research attempts to develop explicit causal explanations of the complex social, organizational, and inter-organizational phenomena encompassing the IS field (Wynn & Williams, 2008a).

Finally, in order to control the influence of various biases on the research process and the generated results (Wynn & Williams, 2008b) this chapter did not compromise on data triangulation. This was to aid in testing validity through the convergence of information from different sources (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). In this regard, both internal (interviews with the respondents at various times as well as document examination) and external triangulations (interviews with other stakeholders such as officers at the cybercrime unit of the Ghana Police Service, Bankers and internet café operators) were conducted. Further, methodological triangulation through participant observation and website, newspaper reports and document analysis was employed.

Data Collection and Analysis

Both unstructured and Semi-structured interviews were the primary data collection methods employed for this chapter. This was done through several planned and unplanned interviews with the core respondents; perpetrators. In each instance of the interviews, the researchers spent between 45 minutes to an hour with the respondent. However, the researchers asked other spontaneous questions via phone conversation to ascertain clarifications for data collected earlier. The recognised leader of the group holds a senior secondary school certificate with somewhat IT training skills from an IT college in Ghana. He has been practising the act since 2008 and that is sole means of living. Two among the other three also hold senior secondary certificates while the last among them dropped out of secondary school.

Upon obtaining information from the perpetrators the authors then followed up by interviewing six internet café operators, eight bank staff from two major banks in Ghana (one local and one foreign-owned banks), eight lawyers and officials from the cybercrime unit of the Ghana Police Service. This was to verify and obtain their perspectives on the data collected from the case subjects. All interviews were recorded and transcribed for coding purposes. As CR emboldens the use of multiple sources of data collection of perspectives of mechanisms and structures which underpin readily observable events, the researchers conducted observations of interactions among case subjects and their victims.

Mode of Analysis

Critical realism as applied in social research seeks to penetrate social phenomena and disclose deep social structures (Brown, Slater, & Spencer, 2002). Abstraction entails separating the intrinsic and constituent properties in a social phenomenon from contingent ones to find what in the phenomenon makes it what it is and not something else (Boateng, 2014; Danermark et al., 1997). After the data collection, themes (focusing on the events/forms of cybercrime) were generated from the transcribed interviews. Each theme was examined as a critical event towards achieving an outcome. Analytical techniques were drawn from Miles and Huberman (1994) qualitative data analysis approach which identifies three other stages after data collection; data reduction, data display and drawing conclusion and verification.

FINDINGS, ANALYSIS AND DISCUSSION

1

This section presents the case finding of the chapter. For purposes of confidentiality, the name of the leader will be referred to Chief informant and their collective name as *the Group*.

Cyberculture Among Ghanaian Youth

As indicated in the foregoing paragraphs ICT and for that matter internet penetration in Ghana has been on the ascendancy. Prior to this, internet cafés in the country became extremely popular in Ghana possibly to afford citizens who cannot afford dedicated internet services the opportunity to temporary use the cafés at a fee. An Earlier study by Burrell (2012) on internet café patronage and usage suggested that the typical Internet user in these cafés – young, educated but not to a university level, and usually not from affluent families – had a different relationship to ‘information’ than older, university educated, and affluent users. The two groups of people identified both have different purposes of using the internet cafés. According to Burrell (2012) the younger groups spend more time in the cafés and usually come in groups pursuing entertainment and occasionally playing computer games. University graduates and students on the other hand patronized the internet cafés to research and acquire information.

The internet cafés served as place where young people are if at all immune to the supervision of their parents. This therefore afforded young patrons of internet cafés the opportunity to gang up at nights after school hours at the cafés for conversations and sometimes arguments about subjects of interests. By so doing, harmless thoughts of looking for pen pals are developed into seeking partners at online dating platforms and thence developing petty cyber-deviant skills. It is worth noting that some cyber deviances are learnt through shared opinions of peers in the cafés. Examples of cyber deviant behaviours among youthful café patrons include identity theft, credit card fraud and online shopping, romance scams among others. It is common knowledge among the youth who patronize the cafés that there are specializations in the abovementioned forms of cybercrime. As such they lend their services among themselves for percentages of the proceeds that emerge from such ventures. It is against this backdrop that a group made up of four members emerged. The ensuing sections present an elaborate picture of one of such group.

Group Profile

The *Group* which began informally with a workforce of seven people in 2015 currently houses four core working group with one female affiliate. At inception, the members of the group patronised the same internet café in their neighbourhood; however, at the time, they operated in *each one for himself* situation. Chief Informant, the leader of the group began engaging in internet crimes in 2008 while in senior high school. He graduated in 2012 and furthered in a reputable IT training school in Ghana. He dropped out of the IT training in 2013 after becoming disappointed in the program. Among the other three in the group, one dropped out of senior high school while the other two completed. The group operates in the Chief Informant’s room. Though the room is not explicitly furnished for office/scam duties, they have acquired two computer desks and office chairs to warrant comfort of operations. At the time the computer desks are occupied, the rest work from a ‘*three in one*’ living room chair and the table placed at the centre of the room. Table 4 below summarises the educational level of the group members as well as their years of experience in perpetrating cybercriminal activities.

Table 4. Education level and cybercrime experience of group members

Pseudo-names	Age*	Educational Qualification	Years of Experience	Formal Work experience
Chief Informant	27	Senior High School Leaver with partial IT training	Since 2008	-
GM2	25	Senior High School Leaver	Since 2011	-
GM3	25	Senior High School Leaver	Since 2011	Electrician
GM3	26	Dropped out of senior high	Since 2013	-

*Ages as at the time of data collection

Prominent among the many activities conducted by the group include confidence romance scams, credit card (generation) fraud, identity theft and online shopping. The scheme of operations in the aforementioned activities has been outlined in the following sections.

Confidence Romance Scams

The ultimate motive of the group is to acquire wealth and as such confidence romance seems to be top of the agenda in that regard. This activity commences by first creating attractive profiles in social media sites especially online dating platforms. In this instance, identities provided are either a rich old man (60 years plus) seeking equal financially sound middle-aged female ‘lover’ or a young philanthropist and financially independent female (usually between 25-35 years) seeking equally rich old men for relationships. They use appealing descriptions such as globetrotter, civil engineers, international social worker undertaking humanitarian projects in Africa among others (see Figure 3).

Such self-descriptions tend to appeal more to women mostly single or divorced who are seeking to begin new relationships. It must however be noted that the scammers create multiple accounts, stalk and send friend requests to one particular target until he/she falls for one of the fake identities (see Figure 4). The scammers begin forging appealing stories about themselves to get the targets glued to the friendship. Here the motive of the scammers is to surge intimacy with the victim with the intention of building trust. In efforts to achieve this, both parties introduce themselves and chat about their past and how they intend to rebuild a lasting relationship.

Sometimes I tell them my former wife left me because I was travelling too much...but now that I want to go back to my country and settle, I need someone as sweet as you. (The Chief Informant)

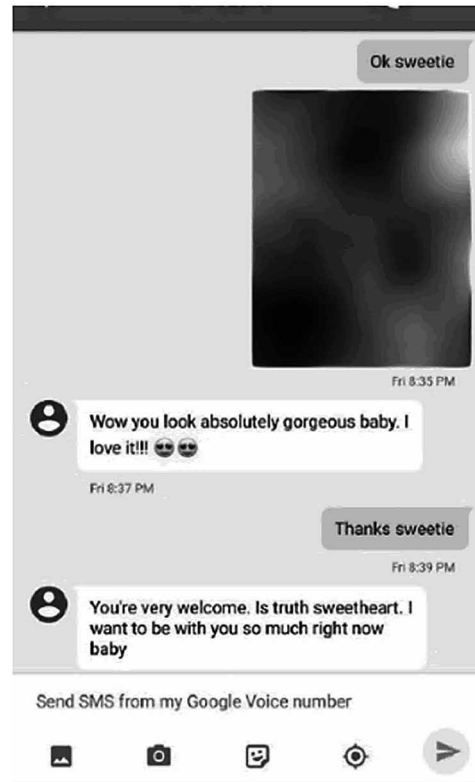
At this stage, the scammers maintain a perfect storyline in order not to lose the relationship. In the words of the Chief Informant, *you have to correctly remember the story for each client*¹.

After establishing trust at this level, the scammers go the extra mile to purchase flowers from online sites to be sent to the would-be victim thereby instilling confidence in them that the relationship is for real. This then opens the way for the exchange of gifts between the two.

After some months of engaging each other, *it is time* for the ‘scammer’ *to go back home* which then requires them to forge a new story inching to the close of the deal. Here the scammer may create a tragic story which will compel the victim to give in to the scam finally.

Figure 3. A snapshot of a conversation between a scammer and would-be victim

1



So, I was robbed on the day that I had to leave back to America by the taxi driver who drove me to the airport. So, I am stranded at the airport right now... even at the time I am chatting with her, I am using the airport police's computer. So, she should send me money for airfare back home (The Chief Informant).

At this stage of the relationship, smart victims or victims who have a wind of how cybercriminals operate abruptly ends the relationship. However, those who fall prey send the monies for the 'scammer' to come home for them to start their family. Here, the scammer requests the victims to send the funds through their assistant since he (scammer) has lost all belongings due to the robbery. The newly introduced assistant in real life in most cases is the real identity of the scammer or the female accomplice.

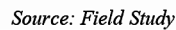
The scammer upon receiving the money ends the relationship and deletes all particulars, pictures and profiles relating to that particular account.

Oh! Sometimes when I receive the money, I tell her to wait for me at the airport and that is the end of it (The Chief Informant).

Credit Card Fraud, Identity Theft and Online Shopping

Data collected during the interview points to the direction that most scammers in Ghana knowing or unknowing engages in multiple internet crimes at a point in time. This emanates from the fact that most of the crimes perpetrated by the scammers are interlaced (see Figure 5). The following paragraphs describe the crime and their interrelationships.

Figure 5. Interrelationship of crimes by scammers

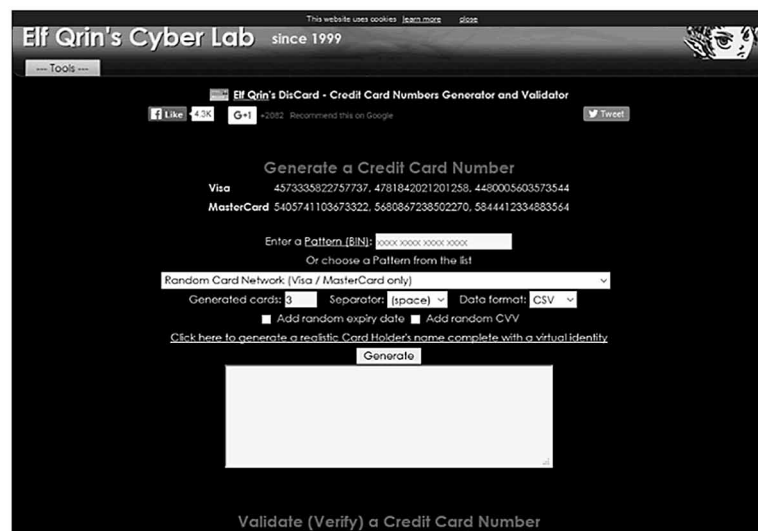


Scammers in registering for exclusive online dating communities are compelled to make payments thereby having to resort to *credit card fraud*. Here, there are various ways scammers do this but only two will be discussed. First, there are credit card generating websites where these scammers generate credit card numbers randomly (see Figure 6). After which they are required to find identities behind the cards. These numbers are then used to register on dating sites to lure women seeking dating opportunities. It must however be noted that registrations on dating sites are to a large extent not intentions to use the site but have linking determinants. Thus, scammers need to test the validity of the credit cards as well as find vulnerable women either to lure or use as conduits (unknowingly) for their fraudulent activities.

... if I want her to believe me more, I buy things with the credit card for her so that she will know that I am original ... As for her, she don't know but me, I am testing the card (informant 3).

The second method scammers device in getting credit card numbers is buying from hackers. These are faceless people who hack into bank details and sell cards at a cheaper rate to scammers. In this case, scammers buy bitcoins, perfect money, web money et cetera with their native currencies and use the internet money to buy hacked credit cards from the hackers. The risk involved here is that the credit cards may or may not contain money. However, in instances where the cards contain some amounts of money, the scammers use the real details of the cards to buy from online retail shops such as Amazon, Apple, Walmart, Bestbuy et cetera but the difficulty in this venture is the blacklisting of some countries including Ghana by these shops. This then compels scammers to resort to alternate means and that is by finding lovers/clients on online dating sites who may later fall for their tricks. At this stage, the scammer engages the interest of the client for a long period to win his/her trust. After the trust is won, the client (would-be victim) is told the scammer is organizing a charity initiative in Africa, and that donors would be sending donations to him in Africa however they (the donors) are unable to do so because most shops in the states do not ship directly to Africa. This in effect implies the lover would have to receive all donations and ship them to the home country of the scammer in the name of his personal assistant. It is worth noting also that some clients do not send the donations. Such victim turned scammers also terminate the relationships with the Ghanaian scammers.

Figure 6. Snapshot of Elfqrin credit card generating page



... That one is for JSS people ... we buy the cards from the black market with bitcoin... some of the cards can contain enough money and others too, small money... it is like gambling (Chief informant downplaying the first method).

Other Stakeholder Perspectives of Cybercrime in Ghana

In our quest to triangulate data from the field, eight bankers, six café operators, eight lawyer and officers at the cybercrime unit of the Ghana Police Service were interviewed.

Bankers

The minimum years of service from bankers interviewed was three years. In Ghana for instance, the requirements for one to withdraw or redeem sums of money from international money transfer is any national identification card such as Voter ID, Passport, Health Insurance Cards, Drivers' license. Secondly, recipients are required to fill a form indicating his/her full name, name and address of the sender, the amount he/she is redeeming and finally assess codes. However, there are instances where recipients are required to answer random questions at the request of the sender

When asked if the banks had ever suspected fraudulent withdrawal of monies from their banks, one respondent responded on the affirmative.

Yes, we know when they withdraw money suspected to be fraud monies.

The follow-up inquired of their pre/post-withdrawal actions but the respondent said

There is nothing we can do about it because they present every legal document and fulfil all mandate required of them. In short, we lack the legal evidence to deny them of their withdrawal. One of their tricks is also that they don't come themselves. They send ladies.

Another follow-up was why the bank does not report the suspects for investigations to continue from there. The respondent answered that

Like I said, first of all, we don't hold any legal evidence. Secondly, it will take a long while to conclude. It is usually difficult following such cases especially when the person has met all the requirements to withdraw money.

Regarding efforts to combat cybercrime in Ghana, respondents indicated that on the side of the banks, they ensure maximum security on their online platforms. Therefore, when one makes a transaction online, a pin is sent to his/her phone for confirmation.

Even before you can access another persons' online banking interface, there is a verification code that is sent to the person's phone. So, if it's a third party who is doing that... so it's now a two-way thing. If you don't have your mobile phone, you can't do a transaction online because a verification number will be sent to your phone. Formerly it wasn't like that but because of our reputation, we are trying to bridge all those loopholes and all those gaps to make the system tighter.

Bank respondents finally pointed out to the fact that *the police should be equipped technologically to be able to assess intelligence on cybercrime activities.*

Internet Café Operators

With regards to public internet cafes, the operators indicated that the proliferation of mobile telephony and internet data penetration had disadvantaged their operations. However, cybercriminals are forced to come to their cafés to perform their activities because they do not like operating without pressure. For instance,

Because they buy café time, they need to finish what they are doing before the time runs out. So, they like working under pressure.

They also indicated the multi-stakeholder awareness in the cybercrime phenomenon. They pointed to the fact that the Banks, Police, ISPs and International Shipping agencies are *aware of the thing going on. This thing is no longer illegal oooh. Don't be lied to. I have seen it before; a shipping company's official was tipped GH¢1000.00 for the clearance of a consignment. Who says the police are not aware (he inquired)? A cousin of mine was chased for driving a DV(defective vehicle) plate car but he tipped them for them to leave him. It has become legal but people have turned their blind eyes to it.*

Café operators finally believed, *unemployment* is a major contributing factor to the cybercrime phenomenon. *There are those who want to come out of it but there is an issue with what they are going to do after discontinuing their current venture.*

Legal Practitioners' Perception of cybercrime

The questions in this perspective sought to find out reasons lawyers will or will not defend cybercriminals as well as whether there are laws in the statute books to address this type of crimes. However, they are unaware if there are current state policies on cybercrime. The respondents pointed to the electronic communications act as well as the criminal code of Ghana. On jail term for cybercriminals, one criminal lawyer who had defended a client on sim-box fraud indicated that

One is not guilty until proven guilty and when found guilty, the various acts I mentioned (Electronic, data protection and taxation) provide for custodial sentences where applicable.

Regarding law enforcement and the lack of prosecution of cybercriminals, a litigation lawyer said,

Well, my personal experience with law enforcement agencies with respect to cybercrime is that, cybercriminals are friends with the police... I think that cybercrime is thriving because the police benefits from it. Once they benefit, there is nothing they can do about it.

This assertion corroborates with the internet café operator's claim that *the police are aware of the crime but little has been done to tackle it.*

Cybercrime Unit of the Ghana Police Service

Considering the rate and scope of cybercriminal activities in Ghana, the Ghana Police Service in August 2015 separated the Cybercrime Unit from the Commercial Crime Unit of the Ghana Police Service. Data from the field interview with the officers at the Unit suggested that several elements contribute to the presumed slow efforts to attack cybercriminals. For instance,

Thousands of cases go unreported. Sometimes, the public feels guilty for falling prey to cybercriminals. We are trying to educate our people to empathize with them and not to ridicule them. People do not also know where to report cybercrimes since it's not a conventional crime.

The Officers also pointed out that *we are adequately resourced knowledge-wise. But technologically, we need to be resourced. Even though we rely sometimes on forensics, I must say we are not adequately resourced technologically.*

On laws and policy documents that are used to prosecute cybercriminals, the Official confirmed the claims of the lawyers that,

We rely mostly on the electronic transactions act, the data protection acts and the criminal offences act but to the extreme, we sometimes use a joint charge by combining the acts.

Finally, the police also called for a multi-stakeholder venture in the fight against cybercrime. These must include the ISPs...

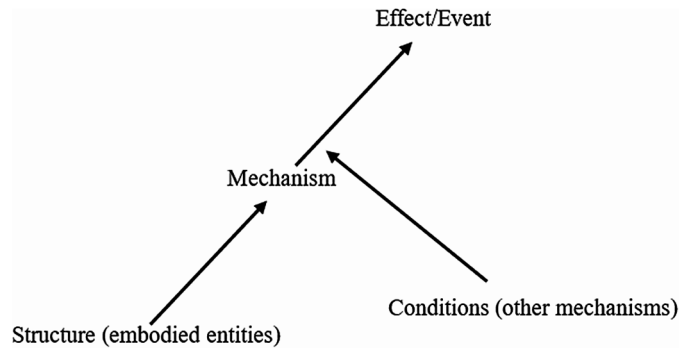
Even though IP addresses are no more static, how prepared are the ISPs to furnish the police with such information.

... the banks must be prepared to report suspicious account revamps to the financial intelligence centre which in-turn investigates and report to us.

DISCUSSION

As illustrated from Figure 7 above, the outcomes of the phenomenon which the researcher seeks to investigate is the event. In the instance of this research, the authors identified the events like the various forms of cybercrimes in Ghana i.e. credit card fraud, confidence romance, identity theft and online shopping (see Figure 8). Even though these events are seen to be independent of each other, cybercriminals combine them as strategies towards an ultimate objective of acquiring wealth. The events are triggered by mechanisms which are dependent on structures (embodied entities) and conditions to occur. Entities or objects provide the essential theoretical building blocks for critical realist explanation and can be such things as organisations, people, relationships, attitudes, resources, inventions, ideas and so on. They can be human, social or material, complex or straightforward, structured or unstructured. Entities have causal powers and liabilities (Easton, 2010). A structure according to (Sayer, 1992:92) can be defined as sets of internally related objects or practices. Entities will usually be structured (Easton, 2010). For

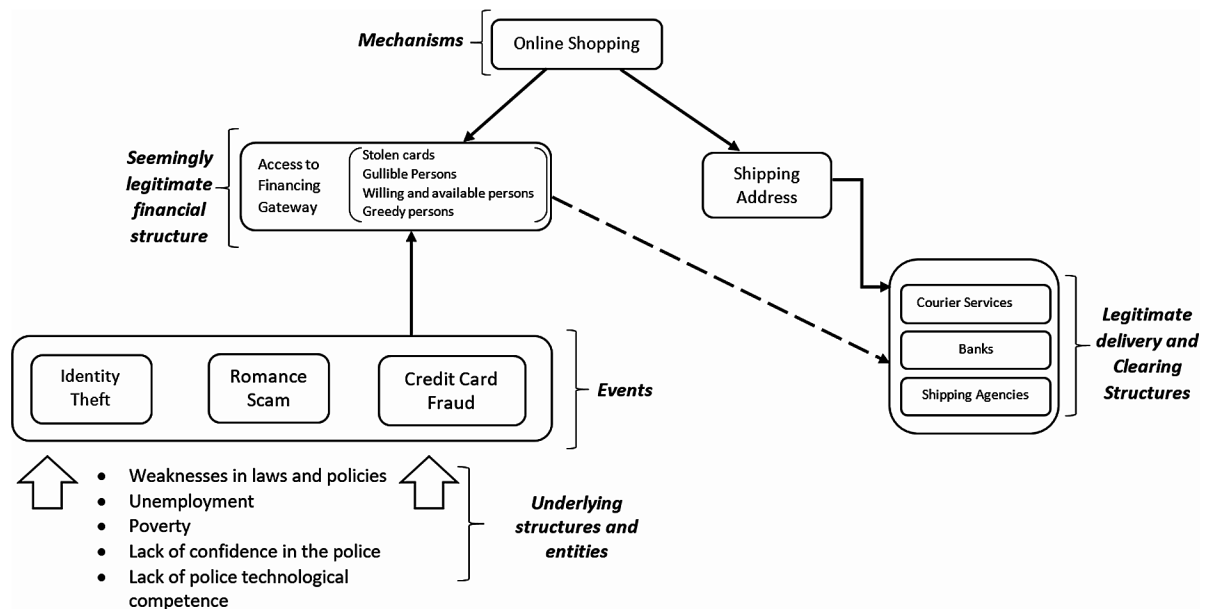
Figure 7. A critical realist view of causation



instance, the case under study consist of a set of entities (people, resources, processes etc.) all of which can affect one another. The aim of a critical realist is to seek causal explanations to a phenomenon i.e. by identifying entities and mechanisms that combine to generate events within specific conditions. Thus, to ask the question “What caused the events associated with cybercrime to occur”. To better explain this, the data has been reduced and displayed in Figure 8 to identify the key entities and conditions which connect and combine within specific mechanisms to generate particular events.

It can be recalled that the routine activity theory postulates three main elements to be present to classify an activity as a crime; motivated offender, suitable target and the absence of a capable guardian. Data collected indeed confirmed this postulation however, our findings pointed to the fact that there exist other factors/elements which contribute in order for cybercrime to take place possibly in the context of our study.

Figure 8. A critical realist view of causation of events



Motivated Offender

The findings from this empirical study suggested that the cybercriminal space is male-dominated. Even though perpetrators sometimes use female accomplices as decoys in withdrawing huge sums of monies from the banks, the majority of the work are done by the male counterparts. Further, the findings suggested that perpetrators are mostly in their young adulthood. For example, a news items read

...The suspects, believed to be part of a wider cybercrime syndicate made up of Nigerians and Ghanaians, attempted transferring a whopping GH¢326 million from the vault of Universal Merchant Bank (UMB) electronically... The ages of the all-male suspects range from 25 to 49 years (Ghana News, 2018).

These findings do not differ from earlier studies which suggest that the perpetrators are young (Aransiola & Asindemade, 2011; Boateng et al., 2011) and that women also do also assist their boyfriends when he is using a female identity (Aransiola & Asindemade, 2011).

The findings of this study finally suggest that cybercrime perpetrators in Ghana arguably include young people who may have been exposed to some level of IT skills in schools. Offenders may as well include school dropouts also with basic IT skills.

Suitable Targets

With regards to the targets of cybercrime perpetrators in Ghana, there seem to be interweaved interests in the target of crimes. For instance, while the offenders may engage a romance victim for a period of time, the scammer's attention is particularly directed at making purchases on online stores through their victims.

The findings of the current study tend to appreciate two of the four-fold (VIVA – Value, Inertia, Visibility and Accessibility) constituents properties of targets classified by earlier studies i.e. the Value and Visibility of targets (Leukfeldt, 2014; Yar, 2005).

With regards to value, data collected was suggestive that place high premium in their targets so much so there are occasional scuffles at public internet cafés. For instance, a café operator recalled that,

There was once a fight here because one guy ran away with another's client... He asked the guy to chat the client for him and later found out that the guy was chatting the client privately on another account.

In that regard, the search for romance victims is tactical in that scammers search for rich and financially sound people desperately looking for relationships.

Concerning the third property visibility, findings revealed that cybercrime perpetrators are patient with dealing with their victims hence creating trust which in turn get victims committed to the relationships. This finding confirms Bennett (1991) assertion that visibility influences an offending decision by allowing the offender to know that a potential target is susceptible; for an object to be targeted, an offender must know it's there.

Finally, evidence from the case points to the fact that the majority of defrauded persons tend to be people who are somewhat easily persuaded to believe the lies the scammers tell them. This attribute coupled with slow reaction from such targets make them victims of scams.

Absence of Capable Guardian

While some previous studies have considered guardianship from a digital point of view (Choi, 2008) others also perceive it as the presence and the capabilities of persons and objects to prevent crime from occurring (Tseloni, Wittebrood, Farrell, & Pease, 2004). Findings from our study is suggestive that cybercrime perpetrators explore the weaknesses in existing laws to commit online crimes. For instance, lawyers and public officials interviewed for this study were of the view that the country lacks the requisite legal and regulatory frameworks in dealing with cybercriminal offences. This finding lends credence to Boateng et al., (2011) claim that Ghana is yet to enact any law to address these forms of crime specifically. Cybercrime prosecution relies grossly on existing electronic, data protection and criminal offences acts.

This chapter further brought to the fore that offenders commit online crimes with the confidence that the police and agencies responsible for clamping down on cybercriminal activities lack the capabilities to do so i.e. they believe the authorities live in a different world with no technical knowledge of tackling the phenomenon head-on. Previous researches have emphasised on the need for law enforcement agencies to be technologically oriented in dealing with internet crimes (Boateng et al., 2011; Olayemi, 2014). Olayemi (2014) for instance posited that laws to combat cybercrimes are useless if law enforcement agencies do not have the education and training necessary even to operate a computer.

Some interesting finding from this construct was that family members of the perpetrators are aware of the acts committed by their relatives. An internet café operator disclosed that *a parent of a 14-year-old boy has been paying for the boy to chat clients... as late as after 10:00pm*. This therefore questions whether internet café operations can be regulated as a starting point toward combating cybercriminal activities in Ghana.

Regarding digital guardianship, cybercrime perpetrators find ways of dealing with anonymity both by their victims and other users of public cafés. First, they install VPNs on the computers they use at the café in order to give them the leverage of choosing their browsing locations. Secondly, they clear browsing data after using public internet cafés. They do so because users who come after them may go into browsing history and retrieve visited websites for personal gains. These findings are contrary to previous literature which have discussed digital guardianship (Bowles, 2012; Choi, 2008; Holt & Bossler, 2014; Howard, 1997; Reyns et al., 2011; Wall, 2008). These contradictions in the findings underscore the need for further studies into digital guardianship of cybercrime in the Sub-Region.

Finally, findings indicated that offenders collaborate with guardians (police, shipping agents, café operators, bankers etc.) in the commission of internet crimes. This manifest in different sections of the data presented where a lawyer alleged that *cybercriminals are friends with the police*. This was reiterated by a café operator who said *I have seen it before; a shipping company's official was tipped GH¢1,000.00 (\$200.00) for the clearance of a consignment*. This comes to confirm Aransiola and Asindemade (2011) claim that offenders' strategies include collaboration with security agents and bank officials, local and international networking.

Technology and Internet Mediation

Existing research have questioned the tenets of the routine activities theory in explaining online crimes (Eck & Clarke, 2003; Reyns, 2013). Reyns (2013) for instance suggested that critical theoretical concepts such as guardianship and target attractiveness take on new meanings in cyberspace, which necessitates adapting the concepts to online environments. Eck and Clarke (2003) also in their view noted that the theory could be expanded to accommodate actions at a distance by making one modification i.e. if the

offender and the target are on the same network. These suggestions manifested in the findings of this research in that, perpetrators of cybercriminal offences rely heavily on internet connectivity to get in touch with their victims. Again, coming from the data, case subjects ensured uninterrupted service by subscribing to private broadband service at their centre of operation. Secondly, there is a heavy reliance on technologies in committing the crimes described in the findings of this study. In romance scams for instance, computers and mobile phones play important essential roles from the search of a victim through to the termination of the relationship. It is against this backdrop that this chapter conceptualises the routine activities theory to include mediating technologies and network as represented in figure 8 below.

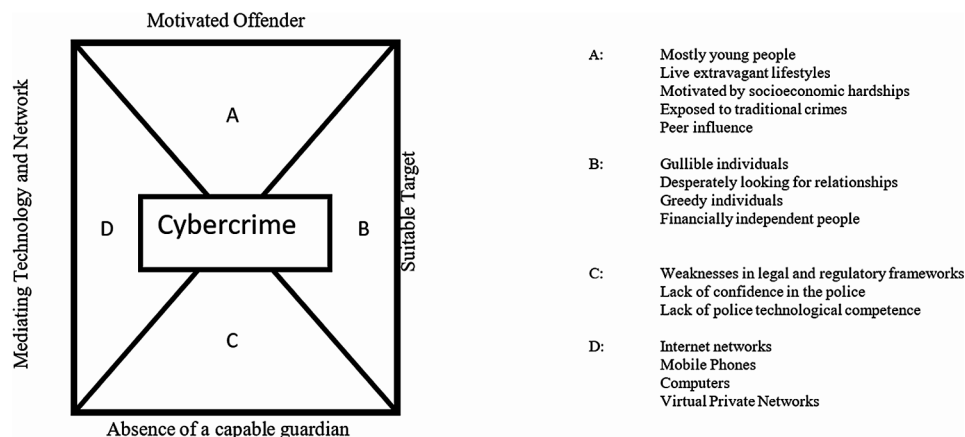
The Routine Activity Theory Revisited

Our conceptualisation of the theory just like Eck and Clarke (2003) is in support of the need to consider the role of networks in the commission of crimes however the influence of technology cannot be discounted (see Figure 9).

Motivated offenders consist of young people mostly between 18 and 40 who seek to exhibit extravagant lifestyles. Offenders are also motivated by certain socioeconomic factors which may include but not limited to unemployment, the desire to lift their families out of poverty, peer influence, exposure to traditional crimes among others. Others may also consist of those who are sponsored by parents to engage in internet crimes. This then leads the discussion to the absence of capable guardians. Capable guardians are made up of any obstructions to the commission of cybercrimes. These may include police, laws, legal and regulatory frameworks, parents, bystanders etc. The absence of this element serves the offender enough motivation to commit internet crimes. Further, cybercriminals thrive on the notion that the police are not adequately equipped to combat electronic crimes in the country.

In relation to suitable targets, cybercrime offenders are more attracted to rich and financially independent people. These people are mostly slow to identify scam relationships and tend to believe in what they are told by the scammers easily. Their delayed reaction and unwillingness to report cybercriminal cases also create opportunities for offenders to thrive. Victims of cybercrimes are sometimes used as transits for online shopping crimes.

Figure 9. Revised routine activity theory of cybercrime



Our primary argument for the modification of the theory comes from the fourth side; mediating technology and networks. Cybercrime arguably flourishes on the internet and as such, certain technologies such as mobile phones and computers are needed to make the cybercrime triad complete. This side of the square according to our findings must be present in order for crime to occur. For instance, offenders rely on the aforementioned technologies to commit internet crimes. Secondly, the migration from target to victim also depends upon the availability of the subject/victim online activities. This therefore demands the presence of the mediating technologies and networks. On the path of the guardian, data from the study suggested that the police needed to be equipped *technologically*; both skills and equipment. These paradoxes accentuate the need for further studies into conceptualising the routine activity theory in relation to technologies and mediating networks in cybercrime studies.

CONCLUSION

The discussion about combatting cybercrime in Ghana as indicated in the research does not seem to be fading any time soon. Even though from all indications, all stakeholders are pointing to the police to spearhead the fight against cybercrime, there requires a multidimensional consensus against cybercriminal activities.

In relation to policy, this research provides adequate findings for the Government of Ghana as well as law enforcement agencies responsible for enacting laws to expedite ongoing processes in formulating policies and laws to govern malicious use of the internet among Ghanaian youth. As evident with other ICT policies and acts such as the electronic transactions act and the data protection act, it has become necessary for civil organizations and individuals to advocate for these laws and regulations to come into being. The chapter also provides adequate findings to inform law enforcers about the modus operandi of cybercriminals. This will aid in the ongoing collaborative discussions between the ITU, Regional Development Forum (RDF) and the Government of Ghana.

With respect to practice, the police must well be resourced both technologically and with qualified personnel in the quest to combat cybercrime in Ghana. This chapter also forms a strong basis for banks, internet service providers as well as shipping and clearing agencies to collaborate with the police in the crack-down of cybercriminals. Finally, on practice, there is the need for ISPs to trace and close down cafés or deactivate mobile internet numbers which are suspected hubs of cybercriminal activities.

With regards to research, this chapter has argued for the revision of the routine activity theory to include mediating technologies and networks; hence viewing the theory from a sociotechnical lens. This research further sought for a multi-stakeholder perception of cybercrime in Ghana and revealed that there were personal or organizational gains in the nosedive of the fight against cybercrime in Ghana. This calls for a comparative research in two different countries; one with a high internet penetration rate and the other with a lower penetration rate. The research also employed a qualitative approach to analyse the multidimensional perception of the crime in Ghana. A different finding may be arrived at if the same study is conducted quantitatively.

REFERENCES

- Alanezi, F., & Brooks, L. (2014). *Combatting online fraud in Saudi Arabia using general deterrence theory*. GDT.
- Ananthakrishnan, U., Li, B., & Smith, M. (2015). *A tangled web: Evaluating the impact of displaying fraudulent reviews*. Academic Press.
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. doi:10.1089/cyber.2010.0307 PMID:22007957
- Bankole, F. O., & Bankole, O. O. (2017). The effects of cultural dimension on ICT innovation: Empirical analysis of mobile phone services. *Telematics and Informatics*, 34(2), 490–505. doi:10.1016/j.tele.2016.08.004
- Bennett, R. R. (1991). Routine activities: A cross-national assessment of a criminological perspective. *Social Forces*, 70(1), 147–163. doi:10.2307/2580066
- Biswas, B., Pal, S., & Mukhopadhyay, A. (2016). *AVICS-Eco framework: An approach to attack prediction and vulnerability assessment in a cyber Ecosystem*. Academic Press.
- Boateng, R. (2014). Resources, electronic-commerce capabilities and electronic-commerce benefits: Conceptualizing the links. *Information Technology for Development*, 22(2), 242–264. doi:10.1080/02681102.2014.939606
- Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa-cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, 11(2), 85–100.
- Bowles, M. (2012). The business of hacking and birth of an industry. *Bell Labs Technical Journal*, 17(3), 5–16. doi:10.1002/bltj.21555
- Brown, A., Slater, G., & Spencer, D. A. (2002). Driven to abstraction? Critical realism and the search for the ‘inner connection’ of social phenomena. *Cambridge Journal of Economics*, 26(6), 773–788. doi:10.1093/cje/26.6.773
- Burrell, J. (2012). *Producing the Internet and Development: an ethnography of Internet cafe use in Accra, Ghana*. The London School of Economics and Political Science (LSE).
- Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5), 545–547. doi:10.1188/14.ONF.545-547 PMID:25158659
- Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1).
- Cohen, L. E., & Felson, M. (1979). On estimating the social costs of national economic policy: A critical examination of the Brenner study. *Social Indicators Research*, 6(2), 251–259. doi:10.1007/BF00343977

Cox, R. W., Johnson, T. A., & Richards, G. E. (2009). Routine activity theory and Internet crime. *Crimes of the Internet*, 302–316.

Cross, C. (2018). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In *The Palgrave handbook of criminology and the global south* (pp. 261–280). Springer. doi:10.1007/978-3-319-65021-0_14

Cybersecurity Ventures. (2017). *2017 Cybercrime Report*. Author.

Danermark, B., Ekström, M., Jakobsen, L., & Karlsson, J. C. (1997). Generalization, scientific inference and models for an explanatory social science. *Explaining Society: Critical Realism in the Social Sciences*, 73–114.

Danquah, P., & Longe, O. B. (2011). Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact*, 11(3), 169–182.

Downward, P., & Mearman, A. (2006). Retrodution as mixed-methods triangulation in economic research: Reorienting economics into social science. *Cambridge Journal of Economics*, 31(1), 77–99. doi:10.1093/cje/bel009

Durkin, K. F., & Brinkman, R. (2009). 419 FRAUD: A crime without borders in A postmodern world. *International Review of Modern Sociology*, 271–283.

Easton, G. (2010). Critical realism in case study research. *Industrial Marketing Management*, 39(1), 118–128. doi:10.1016/j.indmarman.2008.06.004

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies*, 16, 7–40.

Forbes. (2017). *The True Cost Of Cybercrime For Businesses*. Retrieved July 13, 2017, from Forbes website: <https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#16c370584947>

Frempong, G. (2012). *Understanding what is Happening in ICT in Ghana: A Supply-and Demand-side Analysis of the ICT Sector*. Academic Press.

Ghana News. (2018). *CID Arrests 12 suspects of a cybercrime syndicate*. Retrieved September 15, 2018, from Ghana News website: <http://ghananewsonline.com.gh/cid-arrests-12-suspects-cybercrime-syndicate/>

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20–40. doi:10.1080/01639625.2013.822209

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, 46(1), 189–220. doi:10.1111/j.1745-9125.2008.00101.x

Hootsuite. (2018). *The global state of digital in 2018—from Argentina to Zambia*. Author.

Howard, J. D. (1997). *An analysis of security incidents on the Internet 1989-1995*. Carnegie-Mellon Univ Pittsburgh PA.

ITU. (2012). *Understanding Cybercrimes: Phenomena, Challenges and Legal Response*. International Telecommunication Union.

ITU. (2015). Global Cybersecurity Index & Cyberwellness Profiles. In 4. *Lain-Lain*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Jaishankar, K. (2008). Space transition theory of cyber crimes. *Crimes of the Internet*, 283–301.

Jansen, J., & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In *Socio-Technical Aspects in Security and Trust (STAST)*, 2015 Workshop on (pp. 24–31). IEEE.

Ju, J., Cho, D., Lee, J. K., & Ahn, J.-H. (2016). *An Empirical Study on Anti-spam Legislation*. Academic Press.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, 30(4), 470–486. doi:10.1177/0894439311422689

Kolini, F., & Janczewski, L. (2017). Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies. *PACIS 2017 Proceedings*.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, 52(12), 141–144. doi:10.1145/1610252.1610288

Kshetri, N. (2017). *Cybercrime Firms' Internationalization Strategy and Tactics: An Exploratory Framework*. Academic Press.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551–555. doi:10.1089/cyber.2014.0008 PMID:25080013

Longe, O. B., & Chiemeké, S. C. (2008). Cyber Crime And Criminality. In *Nigeria: What Roles Are Internet Access Points In Playing?* Academic Press.

Mason, J. (2002). Sampling and selection in qualitative research. *Qualitative Research*, 120, 144.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Mingers, J. (2004). Realizing information systems: Critical realism as an underpinning philosophy for information systems. *Information and Organization*, 14(2), 87–103. doi:10.1016/j.infoandorg.2003.06.001

National Communications Authority. (2017). *Workshop on Cybercrime Statistics Opens in Accra*. Author.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, 32(1), 81–94. doi:10.1080/02732173.2012.628560

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3), 116–125. doi:10.5897/IJSA2013.0510

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3), 267–296. doi:10.1177/0022427810365903

Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computing in Science & Engineering*, 2(6), 98–100. doi:10.5923/j.computer.20120206.03

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216–238. doi:10.1177/0022427811425539

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, 60(10), 1119–1139. doi:10.1177/0306624X15572861 PMID:25733745

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(11), 1149–1169. doi:10.1177/0093854811421448

Riek, M., Abramova, S., & Böhme, R. (2017). *Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior*. Academic Press.

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), ty004. doi:10.1093/cybsec/tyy004

Sayer, A. (1992). *Method in social science* (2nd ed.). Routledge.

Scott, S. V., Zachariadis, M., & Barrett, M. (2013). Methodological implications of critical realism for mixed-methods research. *MIS Quarterly: Management Information Systems*, 37(3), 855–879. doi:10.25300/MISQ/2013/37.3.09

Strong, D. M., & Volkoff, O. (2010). Understanding Organization—Enterprise system fit: A path to theorizing the information technology artifact. *Management Information Systems Quarterly*, 34(4), 731–756. doi:10.2307/25750703

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The ‘yahoo plus’ phenomenon. *Human Affairs*, 23(4), 689–705. doi:10.2478/13374-013-0158-9

Tapanainen, T. (2017). *Sense-making in Cyber Security—Examining Responder Behaviors in Cyber-Attacks*. Academic Press.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. *21st Century Criminology: A Reference Handbook*, 1, 279–287.

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology*, 44(1), 66–91. doi:10.1093/bjc/44.1.66

- van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407–412. doi:10.1089/cyber.2017.0028 PMID:28657783
- Wada, F., Longe, O., & Danquah, P. (2012). Action speaks louder than words-understanding cyber criminal behavior using criminological theories. *Journal of Internet Banking and Commerce*, 17(1), 1–12.
- Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers & Technology*, 22(1–2), 45–63. doi:10.1080/13600860801924907
- Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, 5(1), 736.
- Wynn, D., & Williams, C. (2008a). Critical Realm-Based Explanatory Case Study Research in Information Systems. *ICIS 2008 Proceedings*. Retrieved from <http://aisel.aisnet.org/icis2008/202%5Cnhttp://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=icis2008%5Cnhttp://aisel.aisnet.org/icis2008/202/>
- Wynn, D., & Williams, C. (2008b). Critical Realm-Based Explanatory Case Study Research in Information Systems. *ICIS 2008 Proceedings*.
- Wynn, D., & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *Management Information Systems Quarterly*, 36(3), 787–810. doi:10.2307/41703481
- Xiao, B. S., Chan, T. K. H., Cheung, C. M. K., & Wong, R. Y. M. (2016). An Investigation into Cyberbullying perpetration: a routine Activity Perspective. *PACIS*, 370.
- Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407–427. doi:10.1177/147737080556056
- Zhang, J., Lee, G., & Wang, J. (2016). *A Comparative Analysis of Univariate Time Series Methods for Estimating and Forecasting Daily Spam in United States*. Academic Press.

ENDNOTE

- ¹ Client is the name given to the victims. Other names scammers call victims include *Mugu* (mostly for men).

Left-Wing Extremism From the Indian Perspective: An Econometric Interpretation

1

Sovik Mukherjee

St. Xavier's University, Kolkata, India

INTRODUCTION

Background and Motivation from the Existing Literature

To put in simple words, Left-wing terrorism (also sometimes called as Marxist–Leninist forms of revolutionary terrorism) is an action of revolt undertaken “to overthrow conservative or capitalist systems and replace them with the Marxist–Leninist or socialist societies.” (Gupta et al., 2004). However, LWE activities are not only common to capitalist regimes but even socialistic regimes have seen LWE occurring within their domestic territory against the ruling government. It has taken vivid manifestations across the world and presented diverging dynamics and relationships (Aubrey, 2004) with national governments and political economies. India is no exception.

A force centric anti-LWE policy has gained ascendancy under the current regime in New Delhi. The government has attempted to focus on increasing the capacities of the forces, undertaking proactive operations to neutralize top extremist leadership. However, like its predecessor, even the government, at present, has struggled to implement such a policy that is wracked by a range of deficiencies. The problem still persists. One of the serious problems in this regard is the lack of coordination between the police force and the CRPF. Following the April 2017 Chhattisgarh attacks, reportedly, there were issues raised as to why the police force did not cooperate with the CRPF. The UPA government had created United Command (UC) structures in four different states - Chhattisgarh, Jharkhand, Odisha and West Bengal - to establish coordination between the various forces who take part in these anti-LWE operations. It was later revealed that the UC structures did not meet every six months, as per the norms and guidelines laid down, but as per the convenience of the concerned authorities and mostly, after a major attack. It is to be noted that a meeting of the UC in Chhattisgarh took place in May 2017, after a gap of 15 months and was convened only after two major attacks by the extremists in March and April 2017 (Routray, 2017).

From the security force point of view, a popular theory has been around for a while prescribing a solution to the LWE problem. It says the CPI-Maoist can be defeated only by sustained deep penetrating operations into the core extremist stronghold areas. While this can certainly provide a solution to the military nuisance of the CPI-Maoist, somehow most state administrations have managed to elicit only a partial involvement of the civil administration whose role in these areas assumes critical importance. States over the years have indeed taken gradual steps to increase the writ of the state into the hitherto LWE dominated areas (Suneja, 2018). As Routray (2017) points out, in Chhattisgarh, there have been new security posts coming up in places like, Kistaram-Golapalli (Sukma) and Bhadrakali (Bijapur) and the Bastar range now has 14 helipads equipped for night landing of choppers used mostly for logistical duties. It is a matter of great pride that such moves have indeed been successful despite extremists at-

DOI: 10.4018/978-1-5225-9715-5.ch006

tempts to mount repeated attacks on the security forces setting up such camps and also public relations campaigns urging tribals to undertake ‘*Police Camp Bhagao Andolan*’ (movement to chase away police camps). Also, other measures initiated by New Delhi for the LWE affected areas include road connectivity projects, mobile connectivity through installation of mobile towers, making education and skill education accessible by initiatives like Rashtriya Madhyamik Shiksha Abhiyan (RMSA), Sarva Shiksha Abhiyan (SSA), establishing Kendriya Vidyalaya (KVs) in the affected districts, opening up of banks, ATMs, etc. to be able to make inroads into the extremist dominated areas. Given such initiatives, the contribution of the paper lies in econometrically estimating the extent to which these developmental factors affect the occurrence of LWE activities.

Thus, Left Wing extremism (henceforth, referred to as LWE)¹ has emerged as one of the major security challenges that India faces. This cannot be a mere manifestation of the prolonged state-building process that the states within the region have been undergoing but rather a movement towards dismantling the existing disproportionate socio-economic and political structures established for catering to the interests of the upper strata of the society. The relative success that these groups have been able to achieve varies from place to place and group to group. Despite shrill assessments across the board and an enveloping sense of apprehension promoted by polarizing politics, the past year has been astonishingly peaceful in India in terms of terrorist and insurgent violence. Total terrorism/insurgency related fatalities across India at 411 (see Table 1), are at a dramatic low - certainly, the lowest since 1994. Indeed, since 2012, total fatalities across the country have remained below the ‘high intensity conflict’ threshold of a thousand fatalities per year. It is useful to recall that fatalities remained above 2,000 for 18 of these 22 years; out of which they were above 3,000 for 11 years; above 4,000 for five years; and just over 5,000 only in 2001. The cumulative totals of the multiple insurgencies in India’s **troubled Northeast**, similarly, remained above the ‘high intensity’ threshold in 2007 and 2008, but have declined enormously since then. As projected, the dramatic contraction of Left Wing Extremism (LWE) – in terms of geographical areas of influence and violence has primarily been the result of successful intelligence-based operations launched by the Security Forces (SFs) over the past years, which have helped neutralize top cadres among the rebels. According to the SATP database, between 2010 and 2016, at least 677 leadership elements of the Maoists have been neutralized (84 killed, 391 arrested and 202 surrendered). To name a few of the initiatives, according to the Union Ministry of Home Affairs (UMHA) data, the total number of LWE cadres arrested between 2010 and 2015 stands at 11,608. At least 633 LWE cadres surrendered

Table 1. Trend in deaths on account of LWE activities in the last 5 years

Year	Civilians	Security Forces	Terrorists/Insurgents/Extremists	Total
2020 (E)	101.8	62.8	275.6	437.8
2019 (E)	104.1	65.5	249.8	417.8
2018	106.0	75.0	230.0	411.0
2017	109.0	76.0	150.0	335.0
2016	123.0	61.0	251.0	435.0
2015	90.0	59.0	110.0	259.0
2014	127.0	97.0	121.0	349.0
Total*	555.0	368.0	862.0	1789.0

Source: Compiled from the South Asia Terrorism Portal

Note: E stands for estimated; A basic linear trend relationship of the form $y_t = \alpha + \beta t$ has been used for forecasting.

*: Total is only from the actual figures i.e. from 2014-2018

over the same period. As SFs establish dominance the erstwhile areas of LWE dominance, efforts at the level of civil consolidation have also increased. UMHA has now claimed the implementation of the Fortified Police Stations (PSs) scheme for construction/strengthening of 400 Police Stations in 10 LWE affected States at INR two million per Police Station on a funding pattern of 80 per cent (Central share): 20 per cent (State share) basis. Also, the Ministry of Road Transport and Highways (MoRTH), under the Road Requirement Plan-I (RRP-I), across eight states of India, has constructed 3,904 kilometers of roads (till 31st of January, 2016). However, in the Indian context, the empirical literature remains under-developed (see Mazumdar, 2013; Pillai, 2010; Basu, 2011; among others). The author pitches herein with an econometric model to estimate the impact of socio-economic parameters, poverty and inequality on LWE related deaths.

This paper makes an attempt to contextualize the nature and spread of LWE and the threat it poses to the Indian state. Are the states vulnerable to such attacks experience an inertia effect from the past LWE activities? The rest of the paper has been organized as follows. The current positions of the severely affected states in India have been highlighted and following this, the empirical model has been estimated. The paper finally ends with consequential discussions and future research possibilities thereof.

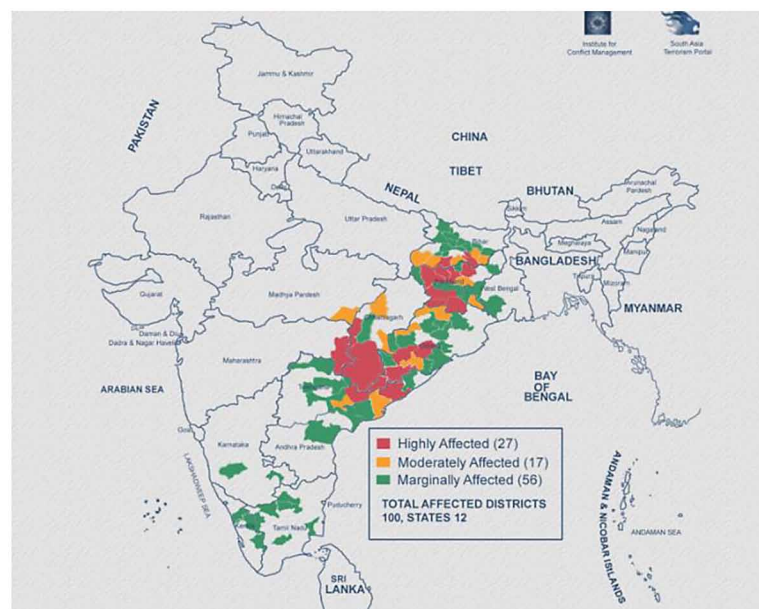
Objectives

It is often a fact that it is this highly disproportionate appropriation of resources across the different sections of the society that is actually the cause of social deprivation which in turn creates the breeding ground for social tension. Furthermore, the causes of social unsustainability are often centred on religion, caste and other divisive factors which may tend to polarize the people. The interaction of the host of such complex factors may thus create problems of social sustainability which would also be having adverse feedback effect on productivity of resources and economic growth.

Figure 1. The extent of spread of Left-Wing Extremist Activities_recent in 2018

Source: South Asia Terrorism Portal;

Note: Based on 2017 data



Against this background, the paper tries to geographically locate the pockets where such forms of crime are the most prevalent and do a trend analysis for these states over a period of five years. In addition to this, the paper models Left Wing extremist activities across twelve severely affected states² in India for a period of nine years from 2008-2017 in a Generalized Method of Moments (GMM) set-up to take care of the endogeneity problem which are quite likely to arise in case of such analysis. In conclusion, the results highlight that while economic growth has a definite positive role in abating such violent forms of left-wing extremist crime, the development strategy should give high priority to literacy, internal security and human development.

CURRENT POSITION OF LEFT WING EXTREMISM ACROSS INDIAN STATES

Extremist activities constitute a source of violence and crime across selected states in India (refer to Figure 1 for the geographical details) in certain regions like Kashmir, certain parts of North Eastern states, as well as in states of Eastern, Central and Southern India like Jharkhand, Bihar, Chhattisgarh, Madhya Pradesh, Odisha, West Bengal, etc.. The form of violence has been mostly of insurgency, terror attacks by poor people mobilized by the political activists who are driven by their political and economic ideology and agenda. The famous terror attacks of Kashmir Valley are mostly driven by political factors and issues of dispute between the Indian states on the one hand and the Pakistani state, Pakistan supported terror groups or the local Kashmiri political-economic entities on the other. The insurgency problem of the Northeast is again attributable to complex regional, ethnic and political issues along with the long neglect of development in the region. However, the motivation of this paper is particularly on the violent terrorist activities of insurgency in certain parts of Eastern, Central and Southern states being driven by mainly Left-Wing Extremist (Maoists or Naxalite or Extremist) groups and not general terrorist attacks *per se*. The pattern of such incidents across the different districts of the states under consideration is highlighted in Table 2 while the projection for India on the whole has been given in Table 1.

As on December 2017, the number of districts affected across 09 states stands at 105. The districts affected by left wing extremism stood at 106 in 10 states as on February 2016.

The journey from when LWE became active in the 1960s till date has been a threatening experience for peace and security. In the 1960s, when it began, LWE concentrations were mostly in the state of West Bengal, areas like Naxalbari, Khoribari, etc.. With the passage of time, basic motivational issues for such forms of extremism like poverty, inequality, social deprivation and discontent among the masses have assumed center stage and now, India's celebrated 'Red Corridor' spreads across ten states as described in Table 3. Their violent agenda and mass outcry against the state, rejecting parliamentary politics has intensified the internal security threat in India, at present — the intensity being higher in states like, Bihar, Jharkhand, West Bengal and Chhattisgarh. If one observes Table 3, this stretch of the 'Red Corridor' starts from India's border with Nepal to the absolute northernmost fringes of Tamil Nadu, including the coastal parts of states like West Bengal and Odisha.

METHODOLOGY

In the existing literature (see for example, Kelly, 2000; Osgood, 2000 among others) the number of occurrence of any type of left-wing extremist activity is a discrete random variable and its average rate of occurrence (λ) is fixed for a defined period. Again, the chance of occurrence of the event at any point of

Table 2. Deaths on account of LWE activities in 2017 for 5 selected states in India (district-wise)

Districts	Civilian	SF	Terrorists	Total
Andhra Pradesh				
East Godavari	1	0	1	2
Vishakhapatnam	4	1	2	7
Vizianagaram	0	0	0	0
Total	5	1	3	9
Bihar				
Aurangabad	0	0	0	0
Banka	0	0	1	1
Gaya	2	0	6	8
Jamui	7	0	0	7
Lakhisarai	4	0	2	6
Munger	0	0	0	0
Nawada	1	0	0	1
Rohtas	1	0	0	1
Total	15	0	9	24
Chhattisgarh				
Bastar	1	1	4	6
Bijapur	3	7	18	28
Bilaspur	0	0	1	1
Dantewada	4	2	9	15
Gariabandh	1	0	0	1
Kanker	8	1	2	11
Kondagaon	1	2	0	3
Narayanpur	3	1	21	25
Rajnandangaon	5	3	8	16
Sukma	6	42	15	63
Total	32	59	78	169
Jharkhand				
Bokaro	2	0	0	2
Chatra	4	0	2	6
East Singhbhum	0	0	1	1
Giridih	4	0	2	6
Gumla	5	0	0	5
Hazaribag	0	0	7	7
Khunti	5	0	4	9
Latehar	3	0	0	3
Palamu	3	0	4	7
Ramgarh	1	0	0	1
Simdega	0	2	3	5
West Singhbhum	2	0	2	4
Total	29	2	25	56
Odisha				
Bargarh	0	0	2	2
Deogarh	0	0	0	0

continued on the following page

Table 2. Continued

Districts	Civilian	SF	Terrorists	Total
Kalahandi	2	0	1	3
Kandhamal	1	1	1	3
Koraput	2	8	1	11
Rayagada	1	0	0	1
Malkangiri	12	0	2	14
Nuapada	0	0	0	0
Sundargarh	0	0	2	2
Total	18	9	9	36

Source: Compiled from the South Asia Terrorism Portal

Note: These data are not deaths due to terrorist activities but deaths due to LWE activities. One should also note that we have excluded Jammu and Kashmir because for the state of Jammu and Kashmir it is very difficult to differentiate out the deaths caused to general terrorist activities from terrorist activities on account of LWE.

Table 3. The districts affected across the states in India

State	Number of Districts in State	Number of Districts Affected	Districts Affected
Jharkhand	24	18	Hazaribagh, Lohardaga, Palamu, Chatra, Garhwa, Ranchi, Gumla, Simdega, Latehar, Giridih, Koderma, Bokaro, Dhanbad, East Singhbhum, West Singhbhum, Saraikela Kharsawan, Khunti, Ramgarh
Bihar	38	11	Aurangabad, Gaya, Rohtas, Bhojpur, Kaimur, East Champaran, West Champaran, Sitamarhi, Munger, Nawada, Jamui
Chhattisgarh	27	10	Bastar, Bijapur, Dantewada, Kanker, Rajnandgaon, Sarguja, Jashpur, Koriya, Narayanpur, Sukma
Odisha	30	9	Malkangiri, Ganjam, Koraput, Gajapati, Rayagada, Mayurbhanj, Sundargarh, Deogarh, Kandhamal
Andhra Pradesh	13	8	Guntur, Prakasam, Anantapur, Kurnool, Visakhapatnam, East Godavari, Srikakulam, Vizianagaram
Telangana	10	8	Warangal, Karimnagar, Adilabad, Khammam, Medak, Nalgonda, Mahbubnagar, Nizamabad
Maharashtra	36	3	Gadchiroli, Chandrapur, Gondia
Uttar Pradesh	75	3	Sonbhadra, Mirzapur, Chandauli
West Bengal	19	3	Bankura, West Midnapore, Purulia
Madhya Pradesh	50	1	Balaghat
Total	319	74	

Source: Press Information Bureau Release, Government of India (2018)

time is independent of when last the event had occurred. It is generally assumed the probability density function of the number of occurrences of such form of crime in a large number of trial experiments of the crime event, is a Poisson density function: i.e.,

$$P(x = k) = \frac{e^{-\lambda} \lambda^k}{k!}$$

Its mean and variance would both be λ .

But, in this model, the author relaxes the assumption of the chance of occurrence of the event at any point of time being independent of when last the event had occurred and introduces an inertia effect. Extending the model proposed by Sengupta and Mukherjee (2018), for any of the individual crime, its average or expected number of occurrence per period is a function of per capita GSDP growth rate, state literacy rate (per cent), size of the police personnel per 1000 units of population, road density of the state per square km. unit, share of minority population (per cent), share of SC/ST population. The double log linear relationship between LWE related deaths and the above mentioned explanatory variables is given below.

We have normalized the measures of some of the variables and/or changed the units of measures in the interest of better presentation or interpretability of the results. For example, we normalize all the relevant variables in per capita terms, or, say, variables like police force size in terms of number per 1000 of population, etc. Again, given the nature of the dependent and independent variables considered, the multiple regression models would often involve endogeneity problems due to the existence of correlation between some of the explanatory variables on the error term of the dependent variable. In view of this we run the Generalized Method of Moments (GMM) to estimate most of the relationships by using the lagged values of such endogenous variables.

If z_i be the crime variable for the i^{th} state, x_j be the j^{th} inequality/poverty variable, y_k be the k^{th} other socio-economic co-variables; influencing the crime variable, the proposed models are the following double log linear ones:

$$\log z_i = \alpha_i + \sum_j \beta_{ij} \log x_j + \sum_k \gamma_{ik} \log y_k + \varepsilon \quad (1)$$

i = Left Wing Extremism related deaths for state i ; j = Gini coefficient (inequality) index, poverty head-count ratio.

k = per capita GSDP growth rate, state literacy rate (per cent), size of the police personnel per 1000 units of population, road density of the state per square km, share of minority population (per cent), share of SC/ST population.

The advantage of using such GMM estimators gets clearly explained when the properties of the estimator does not get distorted when N is small (see Blundell & Bond, 1998; Blundell & Bond, 2000). Moreover, earlier, distribution specific estimators used Monte Carlo simulations where it was not possible to exploit the full set of moment conditions based on instruments when N was small contrary to what happens in this context.

Coming to the estimation procedure, this paper makes use of Generalized Method of Moments (GMM) approach which is superior to Ordinary Least Squares (OLS) and Maximum Likelihood Estimation (MLE) as both in case of OLS and MLE the underlying distribution has to be normal to achieve the desired properties. Moreover, econometric estimation of growth models is usually undermined by the omitted variable and/or the endogeneity problem. There can be an issue of reverse causality which may create biased estimates otherwise. In such a situation OLS fails. The 2SLS estimator, on the other hand, while preferred, is inefficient if there is heteroskedasticity in the data. However, GMM satisfies the properties of efficiency even in case of heteroskedasticity (Siddiquia & Ahmed, 2013). Moreover, system GMM

is a computationally convenient method for estimating a non-linear model without completely knowing the specificity of the probability distribution of data. Here, to take care of the inertia effect, the paper introduces Arellano-Bond estimator. Before starting off, a short technical note needs to be understood first. An unrestricted number of lags of the explanatory variables will introduce a massive number of instruments and eventually, result in a loss of efficiency so following Cameron and Trivedi (2005), there can be a maximum of 4 lags.

However, coming to the decision of considering four lags has been determined by the test of over-identifying restrictions i.e. Hansen's test of over identifying restrictions. The results of which are reported in the next section and are consistent with the statements made by Cameron and Trivedi (2005). Hansen's (1982) J test corrects Sargan's test of over identifying restrictions in the presence of heteroskedasticity. The statistical confirmation of the null hypothesis means the instruments fit the data well but the acceptance of the alternative hypothesis rejects the validity of the instruments (refer to Sargan (1958); Hansen (1982)). The set of assumptions are, $E(\varepsilon_{it})=0$ and $E(x_{it}\varepsilon_{it})=0 \forall t \neq s$.

Coming to the general definition of the Arellano-Bond estimator,

$$\hat{\beta} = \left[\left(\sum_{i=1}^N X_i' Z_i \right) W_N \left(\sum_{i=1}^N Z_i' X_i \right) \right]^{-1} \left(\sum_{i=1}^N X_i' Z_i \right) W_N \left(\sum_{i=1}^N Z_i' y_i \right)$$

and $W_N = S^{-1}$ where,

$$S = \frac{1}{N} \sum_{i=1}^N Z_i' \varepsilon_i \varepsilon_i' Z_i, \text{ where, } \varepsilon : NT \times 1$$

i.e. a set of 8 regressors over 15 time periods.

We have estimated these models with panel data formed out of basic data on violence due to Left Wing Extremism, road density and other developmental factors as obtained from the National Crime Records Bureau of Statistics, road density data per sq km from Road Research Wing of the Ministry of Transport and Highways and other developmental parameters compiled from the Planning Commission and CSO database (see Table 4). It needs to be mentioned that while z_i 's are scalars, the x_i and y_i 's together make it a 1×9 vector (including the constant intercept term) comprising of the regressor variables and their difference levels as given in the specified model equation. When the number of columns in the z_i vector becomes very large, computational considerations may not require the comprehensive use of all possible instruments (see for details Alvarez & Arellano, 1998). In case of a given cross-sectional sample of size N, the use of too many instruments may result in overfitting biases. Given this consideration and following the result of Hansen (1982) test the author sticks to 2 lags and has ignored the least informative instruments.

Primarily, the state response to such LWE activities has suffered due to perceptual differences among the states as well as lack of a unified outlook among the regimes in power. Lack of inter-state coordination and lack coordination between the police and the para-military remains a problem. In some of the tribal areas across states (see Table 3), provision of basic public good services, in terms of education, road connectivity, etc. is lacking which has led to the emergence of Naxalite cadres. Combining development approach with security force operations, emphasis on infrastructural development for road connectivity for human mobility and internal security for peace building should be accorded high priority. Nevertheless, growth with job creation is a necessary condition for a crime free society but not

Table 4. The variable description and the data source

Variable Name/Specifications	Explanation	Data Source
LWE deaths	Number of incidents of violence causing death due to Left Wing Extremism	Crime Records Bureau of Statistics and South Asia Terrorism Portal
GINI Coefficient	To capture the relative dimensions of social tension	Planning Commission Databook, December 2014 and CSO Database
Poverty head count ratio	To capture the absolute dimensions of social tension	Planning Commission Databook, December 2014 and CSO Database
Road density per sq km.	Socio-economic developmental factor	Road Research Wing of the Ministry of Transport and Highways, Government of India
Per capita GSDP growth rate	Socio-economic developmental factor	Planning Commission Databook, December 2014 and CSO Database
State literacy rate	Socio-economic developmental factor	Compiled and interpolated from data available in CENSUS
Size of police personnel	Socio-economic administrative factor	National Crime Records Bureau Statistics
Share of minority population	Socio-economic religious polarization factor	Compiled and interpolated from data available in CENSUS
Share of SC/ST population	Socio-economic factor	Compiled and interpolated from data available in CENSUS

Source: Compiled by the author

sufficient. The sufficiency condition requires appropriate growth policy targeting the proper distribution of the growth benefit, infrastructure development and education and literacy. Education, literacy and per capita GSDP growth are in fact fundamental to abate Left Wing Extremism in India. Law and order solution is necessary but not again sufficient in this context of LWE. The social policies of development should take care of problems of divisiveness due to religion or caste factors in society as riots are found to be sensitive to share of minority or that of SC/ST population and ensure social cohesiveness in our development process. Thus, justifying the choice of variables taken up in this regard.

RESULTS

In order to examine the significance of the impact of the above mentioned explanatory factors on the incidences of violence causing death due to Left Wing Extremism, the author sets up the following econometric models,

Dependent variable is – Number of incidents of violence causing death due to Left Wing Extremism;

Independent variables – Model in Table 6 has Inequality (GINI coefficient) while Model in Table 7 has Poverty (Poverty Head Count Ratio). The other explanatory variables remain the same under both the models which include — road density, literacy rate, growth rate of per capita state gross domestic product, size of police personnel per 1000 population and the vote share of extreme political parties that had contested any form of election in that state concerned in that year.

It may further be noted that the regions (districts) which are affected by poverty and inequality in income distribution also suffer from low level and lack of infrastructural amenities, particularly road connectivity. The latter facilitates terror attacks in the form of insurgency. The geographic maps of for-

est cover, distribution of poverty and that of low level of road density overlap each other in such region. However, the incidences of such Left Wing Extremism are also contingent on the basics of determinants of human development, like education and economic growth which are likely to reduce such crime rates. The development of internal security infrastructure (say size of police personnel) in the state would also tend to abate the incidences of such insurgency related crime committed by the Left Wing extremists.

The basic objective of going for this dynamic panel estimation is to see whether incidences of LWE from the past year consequentially leave behind any kind of inertia effect on the current year LWE activities. Also, if any possibility of endogeneity exists then it would automatically get taken care of through the Arellano-Bond test (Das & Mukherjee, 2018). One needs to clearly understand as to why for small T and large N Arellano-Bond estimator is the preferred estimator. In large-T panels, a shock to the country's fixed effect will make the error term component to decline over time and also the correlation of the lagged dependent variable with the error term will become insignificant (see Roodman, 2009). For combinations of small T and large N panels, this is not necessarily the case and the need for using the Arellano-Bond estimator. The results have been reported in Table 6 and 7.

According to Das and Mukherjee (2018), sometimes the lagged values of the regressors are poor instruments for the first-differenced regressors of equation 1. The Arellano-Bond estimator at the first difference level actually makes these explanatory variables get instrumented with their own lagged values. Before moving on to the discussion of the Hansen test the discussion regarding the two step working mechanism of the GMM estimator, as Das and Mukherjee (2018) have explained, — “There is a two step Generalized Method of Moments method to getting the correct number of lags. First, as an econometric modeller, not only modeling the var-cov matrix under homoskedasticity, but also incorporating the obvious serial correlation in the first difference of the error term components. Next step is to use the residuals from the first step to optimize the weighting matrix which will be consequently used to weight the second stage of the regression.” The results in Table 5 suggest that there is no autocorrelation for higher order lagged values.

The presence of ‘no serial correlation in the first-differenced errors’ as shown in Table 5, at an order higher than 1 means that the moment conditions used by the Arellano-Bond estimator are very much valid. Consequently, after checking with 3 period lagged values as instruments which did not turn out to be significant, the author has used ‘2 period lagged values’ as instruments in this model. Under heteroskedastic data, Eviews 7 package reports the J statistic as distribution of the Sargan test is not known when one deals with heteroskedastic data (Das & Mukherjee, 2018). The model has been estimated based on the Anderson-Hsiao estimator derived from the first-differenced equation, in doing so, instrumenting the lagged dependent variable with the ‘2-time period lagged level values’ of it (Anderson & Hsiao, 1982).

The results in Table 6 and 7, clearly shows that inequality position of the states in India severely affected with LWE activities has a greater intensity in affecting the number of LWE deaths when compared with the poverty head-count ratio. In all the versions of the model considered here, the author makes use of double logarithm Generalized Method of Moments regression method for estimation. Each of the two models have been estimated at the level values of the dependent and independent log variables as well

Table 5. Arellano-Bond test for zero auto-correlation in first differenced errors

Order	z	P > z
1	3.68	0.000*
2	-0.49	0.312

Source: Results as obtained by the authors in Eviews 7; *: denotes significance at 5 per cent level

Table 6. Elasticity estimate of number of incidents of violence causing death due to left wing extremism with respect to causal factors of GINI based social tension along with socio-economic ones

Regression Specification	Double log at levels (including both observed and unobserved state specific effects)	Double log at first difference (removing the unobserved state specific effects)
Independent variables	Coefficients	
1. Inequality variables		
GINI Coefficient	0.78171*	0.1462
2. Other socio-economic variables		
(a) LWE deaths_ (-1)	1.9763*	2.1567*
(b) Road density per sq km	-1.9838*	-2.7499*
(c) Per capita GSDP growth rate	-1.0578*	-0.0631*
(d) State literacy rate	-5.0362*	-4.9856*
(e) Size of police personnel	-0.1729*	-0.1974*
(f) share of minority population	0.2268*	0.4173*
(g) share of SC/ST population	0.9587	0.8862
3. Intercept	51.311	24.627
4. No. of states	12	12
No. of time periods	9	9
5. Sargan test (p value)	0.53*	0.50*

Note: * denotes significant at 95 per cent level;

Source: Results as obtained in Stata 12

Table 7. Model for elasticity estimate number of incidents of violence causing death due to left wing extremism with respect to causal factors of poverty based social tension along with socio-economic ones

Regression Specification	Double log at levels (including both observed and unobserved state specific effects)	Double log at first difference (removing the unobserved state specific effects)
Independent variables	Coefficients	
1. Poverty variables		
Poverty head count ratio	0.5517*	0.0819
2. Other socio-economic variables		
(a) LWE deaths_(-1)	1.7319*	1.9856*
(b) Road density per sq km	-1.1489*	-2.9570*
(c) Per capita GSDP growth rate	-0.7381*	-1.1228*
(d) State literacy rate	-7.9922*	-7.9705*
(e) Size of police personnel	-3.0367*	-2.8185*
(f) share of minority population	0.2951*	0.5022*
(g) share of SC/ST population	0.8767	0.7431
3. Intercept	35.7221	67.3205
4. No. of states	12	12
No. of time periods	9	9
5. Sargan test (p value)	0.50*	0.53*

Note: * denotes significant at 95 per cent level;

Source: Results as obtained in Stata 12

as at their first differences. The inequality or poverty related measures as independent variables have a significant impact on the number of deaths due to such violence. Also, the infrastructural variables like, road and internal security infrastructure in terms of road density per sq km. and number of police personnel per 1000 population tend to reduce such impact on the dependent variable of violent incidents of LWE as expected while the human development factors like state level of literacy have also a significant moderating effect on such events through its impact on overall level of development of the state. Interestingly, the share of minority population has turned out to be a significant factor while the share of SC/ST population remains insignificant. The variables representing the share of minority population or of SC/ST population represents the policy of promoting social cohesion and those of protection of minority as well as dalits are important for peace and cohesion. Moving on, the dynamic panel data model objectively points out to the fact that states having a history of being subjected to LWE terror attacks are vulnerable to such activities. Hence, the inertia effect of terrorism LWE continues to live on i.e. death due to LWE in the past year is directly influencing LWE activities in the in the current year.

However we observe that the results at the first difference level show the impact of the parameter on inequality or poverty as insignificant possibly due to a small sample problem on account of data limitations. We have therefore to use the results of Tables 6 and 7 based on level values of the variates for the policy and other analytic purpose.

CONCLUDING REMARKS AND FUTURE RESEARCH AREAS

The ‘National Policy and Action Plan (NPAP)’ since 2015 launched by the Union Ministry of Home Affairs (MHA) pushes for zero tolerance towards violence coupled with massive efforts put in developmental activities so as to streamline such benefits to the poor and the vulnerable sections in the affected areas. This policy covers 106 districts in 10 states, as already pointed out, which are severely affected by Left Wing Extremism affected. As per NPAP, these districts are covered under the “Security Related Expenditure Scheme (SRE) of the MHA for the purpose of reimbursement of security related expenditure like transportation, communication, hiring of vehicles, stipend for surrendered Maoists, temporary infrastructure for forces etc. to the states”. The reports indicate a substantial decline of around 34 per cent in the number of deaths related to LWE across 58 districts between 2013 and 2017. As a pre-emptive move, the MHA has put tribal areas at the intersection of the states of Kerala, Karnataka and Tamil Nadu under SRE districts. The effectiveness of NPAP in the recent years has brought the list of ‘Most Affected Districts’ to 30, down from 36 — an achievement of some sorts. The policy implications of these results as presented in Table 6 and 7 point out clearly that both inequality and poverty parameters have significant impact with high positive elasticity on such LWE activities. The inequality measure has however relatively higher impact in terms of its absolute elasticity value when compared with the poverty head count ratio. All the other developmental variables including, security related infrastructural connectivity are found to reduce the violent activities by LWE. However, a few points should be noted here:

1. The relative disparity in income and asset distribution, and, not just poverty, has a massive role and significance in accelerating violence of the kind being discussed.
2. Educational attainment and literacy are two of the most important developmental instruments in abating such acts of violence driven by political economic factors.

3. Growth has a special place in the developmental policy of the states concerned. The magnitude of the partial elasticity coefficient of growth, in essence, has a role in eradicating absolute deprivation or poverty but also reducing the inequality among the poor (refer to Table 6 and 7).
4. Last, but not the least, the inertia effect persists from the previous period. The empirical exercise advocates that states having a record of LWE activities will experience such activities, even in the current period. Lower growth in an area having a higher vote share of extreme political parties is an important determinant of political radicalism: a lower growth rate increases the support for extreme political platforms — very true in the Indian context.

The present analysis may be extended in several dimensions. This empirical model has been proposed keeping in mind the Indian context but one can extend it to other developing countries having a history of LWE occurrences. Moreover, India is the largest democracy in the world, so it would be interesting to explore these results for countries having little or almost no experience of democracy. Over a period of time, this model can be effectively used for predicting to what extent the factors considered here are being influenced by the NPAP. Subject to data availability, the scope of further research would be incomplete without tracking down major episodes of natural disasters and calamities, financial and banking crisis, political referendums, etc. and how the results derived in this model change in presence of such factors in a cross-country set-up.

REFERENCES

- Anderson, T. W., & Hsiao, C. (1982). Formulation and estimation of dynamic models using panel data. *Journal of Econometrics*, 18(1), 47–82. doi:10.1016/0304-4076(82)90095-1
- Aubrey, S. M. (2004). *The new dimension of international terrorism*. Zurich: vdf Hochschulverlag AG.
- Basu, I. (2011). Security and development—are they two sides of the same coin? Investigating India's two-pronged policy towards Left Wing extremism. *Contemporary South Asia*, 19(4), 373–393. doi:10.1080/09584935.2010.537745
- Blundell, R., & Bond, S. (1998). Initial conditions and moment restrictions in dynamic panel data models. *Journal of Econometrics*, 87(1), 115–143. doi:10.1016/S0304-4076(98)00009-8
- Blundell, R., & Bond, S. (2000). GMM estimation with persistent panel data: An application to production functions. *Econometric Reviews*, 19(3), 321–340. doi:10.1080/07474930008800475
- Cameron, A. C., & Trivedi, P. K. (2005). *Microeconometrics: methods and applications*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511811241
- Das, R. C., & Mukherjee, S. (2018). Determinants of Terrorism in South Asia: Insights From a Dynamic Panel Data Analysis. *International Journal of Cyber Warfare & Terrorism*, 8(4), 16–34. doi:10.4018/IJCWT.2018100102
- Gupta, S., Clements, B., Bhattacharya, R., & Chakravarti, S. (2004). Fiscal consequences of armed conflict and terrorism in low-and middle-income countries. *European Journal of Political Economy*, 20(2), 403–421. doi:10.1016/j.ejpoleco.2003.12.001

- Hansen, L. (1982). Large Sample Properties of Generalized Method of Moments Estimators. *Econometrica*, 50(4), 1029–1054. doi:10.2307/1912775
- Kelly, M. (2000). Inequality and crime. *The Review of Economics and Statistics*, 82(4), 530–539. doi:10.1162/003465300559028
- Mazumdar, A. (2013). Left-wing extremism and counterinsurgency in India: The ‘Andhra model’. *Strategic Analysis*, 37(4), 446–462. doi:10.1080/09700161.2013.802518
- Osgood, D. W. (2000). Poisson-based regression analysis of aggregate crime rates. *Journal of Quantitative Criminology*, 16(1), 21–43. doi:10.1023/A:1007521427059
- Pillai, G. K. (2010). Left-Wing Extremism (LWE) in India. *Journal of Defence Studies*, 4(2), 1–9.
- Press Information Bureau. (2018). *LWE affected districts*. New Delhi, India: Author.
- Roodman, D. (2009). How to do xtabond2: An introduction to difference and system GMM in Stata. *The Stata Journal*, 9(1), 86–136. doi:10.1177/1536867X0900900106
- Routray, B. P. (2017). *State of Play: Left-wing Extremism in India in 2017*. Retrieved from <http://mantraya.org/state-of-play-left-wing-extremism-in-india-in-2017/>
- Sargan, J. D. (1958). The Estimation of Economic Relationships using Instrumental Variables. *Econometrica*, 26(3), 393–415. doi:10.2307/1907619
- Sengupta, R. P., & Mukherjee, S. (2018). Crime, Deprivation and Social Sustainability—Evidence across States in India. *Indian Journal of Human Development*, 12(3), 1–24. doi:10.1177/0973703018811173
- Siddiqui, D. A., & Ahmed, Q. M. (2013). The effect of institutions on economic growth: A global analysis based on GMM dynamic panel estimation. *Structural Change and Economic Dynamics*, 24, 18–33. doi:10.1016/j.strueco.2012.12.001
- Suneja, K. (n.d.). *Left wing extremism, border tensions challenging for India: Arun Jaitley*. Retrieved from economictimes.indiatimes.com/articleshow/5857661.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

ADDITIONAL READING

- Chandra, U. (2014). The Maoist movement in contemporary India. *Social Movement Studies*, 13(3), 414–419.
- Nayak, N. (2008). Maoists in Nepal and India: Tactical alliances and ideological differences. *Strategic Analysis*, 32(3), 459–475.
- Sarangi, S., & Alison, L. (2005). Life story accounts of Left Wing terrorists in India. *Journal of Investigative Psychology and Offender Profiling*, 2(2), 69–86.
- Thomas, P. N. (2014). The ‘Red Surge’: Media framing of Maoist struggles in India. *The International Communication Gazette*, 76(6), 485–504.

KEY TERMS AND DEFINITIONS

Economic Growth: It can be defined as the increase in the capability of an economy to produce goods and services from one period to another. It can be measured either in nominal terms or in inflation adjusted real terms. Typically, GDP or GNP is taken as a measure of economic growth. In notational terms, GDP growth rate, g_t , $g_t = \frac{GDP_t - GDP_{t-1}}{GDP_{t-1}} \times 100$ where, t indicates the particular time point.

Generalized Method of Moments (GMM Estimation): It is a common method for estimation of the parameters in statistical models. Usually it is applied in the context of semiparametric models, where the parameter of interest is finite-dimensional, whereas the full shape of the data's distribution function may not be known, and therefore maximum likelihood estimation is not applicable. Using the moment conditions, the true parameter values are estimated. The GMM method then minimizes a certain norm of the sample averages of the moment conditions. It is applied in case when there can be a chance of endogeneity problem.

Gini Coefficient: In economics, the Gini coefficient sometimes called Gini index, or Gini ratio, is a measure of statistical dispersion intended to represent the income or wealth distribution of a nation's residents, and is the most commonly used measurement of inequality.

Maoists: Maoists, also known as Naxalites or Naxals, are the group of people who believe in the political theory derived from the teachings of the Chinese political leader Mao Zedong. It is a doctrine to capture State power through a combination of armed insurgency, mass mobilization and strategic alliances. Also, these Maoists use insurgency doctrine based on use of propaganda and disinformation against State institutions. Herein, the author has used Maoists, left-wing extremists, and Naxalites interchangeably.

Monte Carlo Simulations: Monte Carlo simulation is a mathematical technique that generates random variables for modeling risk or uncertainty of a certain system. The random variables or inputs are modelled on the basis of probability distributions such as normal, log normal, etc. Different iterations or simulations are run for generating paths and the outcome is arrived at by using suitable numerical computations.

Panel Data: Also called longitudinal data, represents cross-sectional time series data i.e. data on multi-dimensional cross-sections (comprising of individuals, firms and countries) over a period of time.

Police Force: A body of trained officers entrusted by a government with maintenance of public peace, law and order, enforcement of laws, and prevention and detection of crime.

Poverty Head Count Ratio: The poverty head count ratio (PHCR) is the proportion of a population that exists, or lives, below the poverty line.

ENDNOTES

- ¹ The terms “Naxalites”, “Maoists”, and “Left Wing Extremists” have been used inter-changeably.
- ² The states are Jharkhand, Bihar, Chhattisgarh, Madhya Pradesh, Odisha, West Bengal, Andhra Pradesh, Telengana, Assam, Nagaland, Kerala and Maharashtra. We have not considered any North Eastern state because of lack of availability of data, except for Assam and Nagaland.

Transnational Cybercrime: The Dark Web

Barbara Jane Holland

 <https://orcid.org/0000-0003-3729-0147>

Brooklyn Public Library, USA

INTRODUCTION

The world and human behavior have changed so quickly through the use of technology.

China and India have the largest population of internet users though only 55 percent and 34 percent have total access (Internet live stats 2016). The United States, Brazil, and Japan come next.

The proliferation of technology has clearly led to changes in how individuals engage with the world around them. Today people shop and communicate in digital format.

Most people born in the mid-eighties have never lived without a computer. The endless development of human behavior has created unparalleled opportunities for crime and misuse.

Over the past thirty years, there has been a substantial increase in the use of technology by street criminals and new forms of crime that did not previously exist.

Technology is at the core of information security. It can enable crime, and but also prevent it.

Every country has its own police agency that enforces its own laws. The growth of global transportation systems, international trade, computerized financial transactions, and worldwide availability, of information through the internet have facilitated the expansion of the international economy. These factors simultaneously provided the basis for transnational crime. There is a distinction between profit-seeking transnational crime and international crimes. Which are acts of terrorism, genocide, human rights abuses and other crimes that violate international law (Albanese 2011). Transnational crimes, by contrast, include theft, fraud, counterfeiting, smuggling and other violations of individual countries' criminal laws that involve trans-border activities.

BACKGROUND

Cybercrime involves the use of computers and the internet to commit acts against people, property, public order or morality (de Villiers 2011). Some may occupy a computer to steal funds, information or resources. These thefts can be aimed at stealing money, company trade secrets, chemical formulas, and other information that could be valuable to a competing business. Others may commit destructive acts by releasing a malicious virus or worm to harm a computer system.

Cybercrime is an evolving form of **transnational** crime. The complex nature of the crime as one that takes place in the border-less realm of cyberspace is compounded by the increasing involvement of organized crime groups.

DOI: 10.4018/978-1-5225-9715-5.ch007

Figure 1. Cybercrime



Table 1. World wide web

Surface Web Google, Bing Facebook LinkedIn, eBay, Amazon Illicit online pharmacies Anonymous forums	Deep Web Medical Records Legal documents scientific Reports Academic documents Government documents	Dark Web Mirrored Websites Private Communication Illicit Activity
---	---	---

Transnational Cybercrime can be grouped into three categories. (Albanese, 2011).

The First Category: Provision of illicit goods such as drug trafficking, moving stolen automobiles and artwork, from one country to another for sales, is difficult to trace back to its original owner. (Alderman, 2012). Also included is the transportation and sale of counterfeit goods such as prescription drugs, medication and designer clothing.

The Second Category: Provision of illegal services, includes human trafficking, with the transportation of sex workers or undocumented immigrants illegally into the country(Shamir 2012). Also included are fraudulent investments and child pornography.

The Third Category: Infiltration of business or government. (Albanese 2011). This category includes the widely publicized conclusion by American Intelligence agencies that Russians under the direction of the Russian Government, sought to affect elections in the United States by hacking into American computers and selecting revealing information that would help or hurt certain political candidates. According to the United Nations, the annual profits from Transnational organized crime amounts to 870 billion annually with drug trafficking producing the largest segment of that amount.

Law enforcement official faces huge challenges in combating transnational crime.

THE SURFACE WEB

The magnitude of the web is growing. According to one estimate, there were 334.6 million internet top-level domain names registered globally during the second quarter of 2016. This is a 12.9% increase from the number of domain names registered during the same period in 2015. As of February 2017, there were estimated to be more than 1.154 billion websites.

The Deep Web comprises any content on the web that is not indexed for search engines and that is accessed by password or encryption, or through gateway software. This includes content such as medical records, legal documents, financial records, and government resources. Because this content cannot be searched and indexed, no one knows exactly how large the deep web is, but many estimates place it at 400 to 500 times larger than the surface web.

Deep Web Search Engine

The Torch is one of the most well-known and well-loved deep web search engines there is, and it's also one of the largest. Their index covers more than a million deep web page results. It makes for a great multi-purpose search engine whatever you're looking for.

Popular Deep Web Destinations

- **TorShops:** Start your own deep web store!
- Onion URL Repository
- The WWW Virtual Library
- Tor Links – A list of .onion addresses.
- Facebook
- Hidden Answers
- Dream market
- Sci Hub

THE DARK WEB

The **dark web** is a subset of the **deep web**, which is not indexed by traditional search engines within the Deep Web. The Dark Web is also growing as new tools make it easier to navigate. Individuals may access the Dark Web assuming the little risk of detection, and use this arena for a variety of legal and illegal activities. It is unclear, however, how much of the Deep Web is taken up by Dark Web content and how much of the Dark Web is used for legal or illegal activities

The Dark Web can be reached through decentralized, anonymized nodes on a number of networks including Tor (short for The Onion Router) or I2P (Invisible Internet Project) Tor, which was initially released as the Onion Routing project in 2002. It was originally created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online.

Figure 2. surface, deep and dark web

1

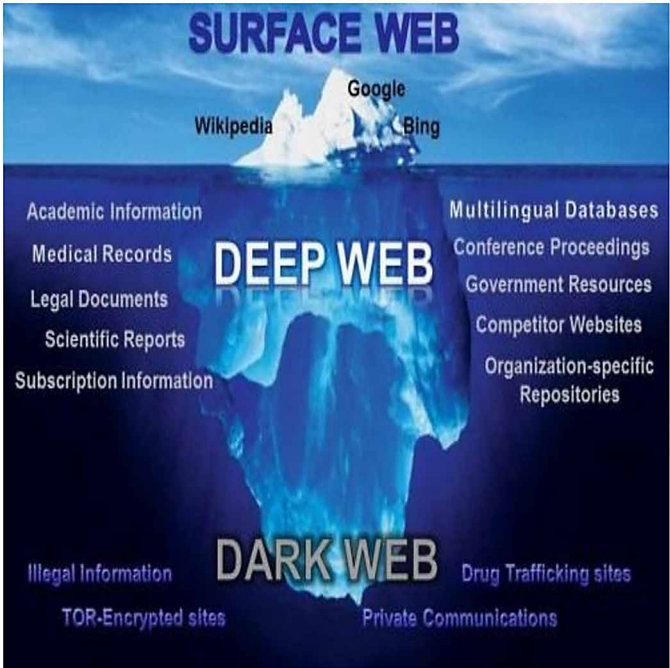
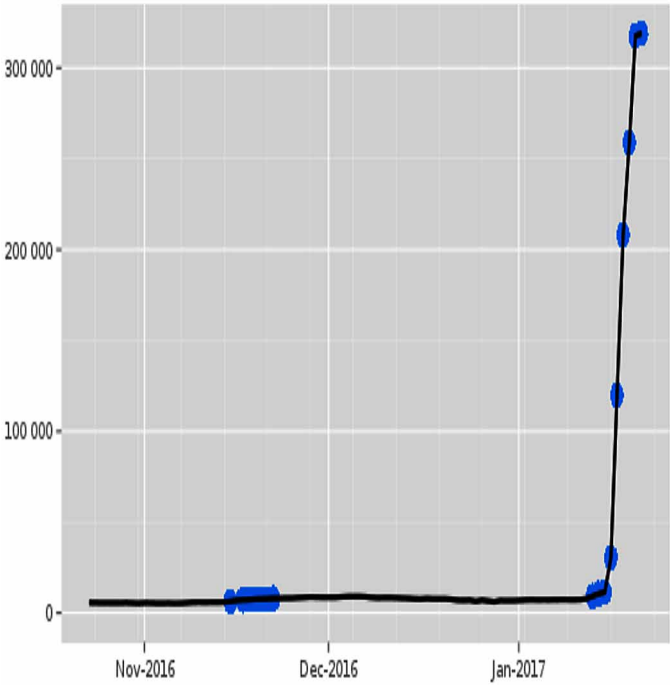


Figure 3. Tor metrics



Popular Dark Web Sites

- The Pulitzer-winning ProPublica. ...
- Facebook's **.onion site**. ...
- Blockchain for Bitcoins on .onion. ...
- Sci-Hub, the world's scientific database. ...
- Netpoleaks is the .onion police monitor. ...
- The Intercept, a .onion SecureDrop with TLS. ...
- Keybase is the cryptographic profile link system
- Flashlight
- Hidden Wiki
- Strategic Intelligence Network
- AnonInbox

The Dark Web and Tor

Tor “refers both to the software that you install on your computer to run Tor and the network of computers that manages Tor connections. Tor’s users can connect to a website through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Users route their web traffic through other users’ computers such that the traffic cannot be traced to the original use or essentially establishes layers (like layers of an onion) and routes traffic through those layers to conceal users’ identities. To get from layer to layer, Tor has established “relays” on computers around the world through which information passes. Information is encrypted between relays, and all Tor traffic passes through at least three relays before it reaches its destination. The final relay is called the “exit relay,” and the IP address of this relay is viewed as the source of the Tor traffic. When using Tor software, users’ IP addresses remain hidden. It appears that the connection to any given website is stemming from the IP Address of a Tor exit relay, which can be anywhere in the world. Although data on the magnitude of the Deep Web and Dark Web and how they relate to the Surface Web is not clear, data on Tor users do exist. According to metrics from the Tor Project, the mean number of daily Tor users in the United States across the first two months of 2017 was 353,753—or 19.2% of total mean daily Tor users. The United States has the largest number of mean daily Tor users, followed by Russia (11.9%), Germany (9.9%), and the United Arab Emirates (9.2%)

Timing Analysis

Utilizing timing analysis, the anonymity of TORs can be broken. One of the reasons typical Internet connections are not considered anonymous is the ability of Internet service providers to trace and log connections between computers. For example, when a person accesses a certain website, the data itself may be secured through a connection like HTTPS such that your password, emails, or other content are not visible to an outside party, but there is a record of the connection itself, what time it occurred, and the amount of data transferred.

1



1



Traffic Analysis

Traffic Analysis can intercept and examine messages in order to deduce information from patterns in communication. This can be performed with messages that are encrypted.

Deanonymization can occur when using end-to-end timing attackers. An adversary monitoring network traffic sent to the initial relay node, as well as traffic sent to the final relay node, can make use of statistical analysis to identify the circuit they belong to. The user's IP address, as well as the destination IP of the observed traffic, can be sniffed by the adversary, who can easily track the clickstream of a user via correlation attacks. The adversary does not need to control the entry and exit nodes within a Tor circuit to be able to correlate network traffic streams observed traveling across these relay nodes. The adversary only needs to be capable of observing the traffic.

Purchasing Drugs and Narcotics Online

The sale of illicit drugs and narcotics has also moved online. The primary resources used by sellers and buyers are on forums operating on the Dark Web which can only be accessed by using specialized encryption software and browser protocols. Individuals can only access these forums using the Onion router or Tor service which is a free proxy and encryption protocol that hides the IP address and location of the users (Barrett, Ferris, and Winstock, 2014; Dolliver, 2015). Moreover, these sites cannot be indexed by Google or other search engines. As a result, this limits the ability of law enforcement agencies to eliminate illicit content because the hosting source cannot be identified through traditional means (Dolliver 2015; Estes 2014).

Silk Road was one of the first Tor-based narcotics markets to gain prominence. The market gained attention from researchers and popular media. Transactions were paid through an anonymous electronic currency called Bitcoins. Law enforcement agencies in The United States and Australia conducted sting operations against the buyers.

Since the opening of Silk Road in 2011, there were over a million transactions worth an estimated 1.2 billion in revenue. An FBI investigation using the handle **Dread Pirate Roberts** led to the arrest of Ross William Ulbricht in San Francisco California October 2, 2013.

Some sites effectively "hidden", have not been indexed by a search engine and can only be accessed if you know the address of the site. Special markets also operate within the dark web called, "darknet markets", which mainly sell illegal products like drugs and firearms, paid for in the cryptocurrency Bitcoin.

Another hidden site called **Assassination Market**, created by Kuwabatake Sanjuro allows users to crowdfund murders through donations of Bitcoin, the anonymous digital currency. The site, which has been up less than a year, is only accessible through the Tor network, currently, lists a total of six bounties, all of which target various government officials. As a result of the dark web's almost total anonymity, it has been the place of choice for groups wanting to stay hidden online from governments and law enforcement agencies. Whistleblowers are known to use the dark web to communicate with journalists, but more frequently it has been used by pedophile groups, terrorists and criminals to keep their dealings secret.

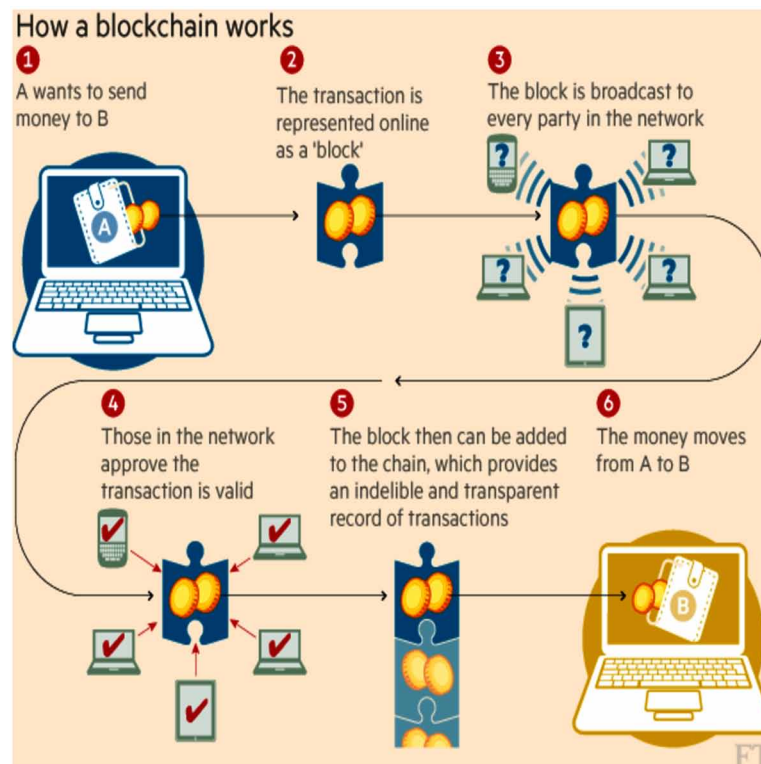
A recent study by Carnegie Mellon researchers Kyle Soska and Nicolas Christin has calculated that drug sales on the darknet total US\$100 million a year. Most, if not all, was paid for in Bitcoin.

Figure 6. Assassination market



1

Figure 7. Blockchain



BITCOIN AND BLOCKCHAIN ON THE DARK WEB

When Bitcoin surfaced, it promised complete anonymity and this caused the global community to embrace it with open arms. However, the nature of blockchain is such that tech-savvy individuals could become privy to the addresses of people making huge transactions on the network. Currently, Cryptocurrencies

like Litecoin and Monero are currently making waves in the market and this is due to the shift from a Bitcoin economy to an altcoin one. These altcoins are more favorable because they process transactions faster and with a certain level of reliability, they also uphold the concept of anonymity better. Their relatively low transaction fees and value also makes it better. The blockchain is an integral part of the dark web and cryptocurrency has been instrumental to its growth.

Sellers and Aliases in the Marketplace

Silk Road became the central dark web marketplace in 2011. Before it was seized by the FBI in 2013; Silk Road 2.0 emerged as the dominating marketplace before being shut down in 2014 in an international effort dubbed Operation Onymous. Evolution then became the leading marketplace before engaging in an exit scam in and was then replaced by Agora, which halted operations as a result of attacks to de-anonymize its server locations. The rise and eventual capture by law enforcement of Alpha Bay and Hans paved the way for the current leader, Dream Market.

November 2014, another San Francisco man by the name of Blake Benthall was arrested and charged with being "Defcon," the Silk Road 2.0 administrator.

Unlike the surface web, a primary function of these dark web marketplaces is to serve as escrow agents between the buyer and the seller, for which the marketplace collects a small fee. Escrow helps to prevent seller and preserves the anonymity of purchases because marketplaces typically tumble the cryptocurrency in the process. Most marketplaces use a technology called multi-signature transactions ("multisig") that require the approval or "signature" of multiple parties in a transaction before payment is released from escrow. 2-of-2 multisig requires both the buyer and seller to sign off before money is released. An increasingly popular option is 2-of-3 multisig, in which two of three parties engaged in a transaction (buyer, seller, and escrow agent) must sign off to release funds.

Following the Silk Road blueprint, modern online anonymous markets run as Tor hidden services, which gives participants (marketplace operators and participants such as buyers and sellers) communication anonymity. Online currencies are used as payment systems (e.g., Bitcoins) to make it possible to exchange money electronically without the immediate traceability that conventional payment systems (wire transfers, or credit card payments) provide.

The common point between all these marketplaces is that they actually are not themselves selling contraband. Instead, they are risk management platforms for participants in (mostly illegal) transactions. The risk is mitigated on several levels. First, by abolishing physical interactions between transacting parties. These marketplaces claim to reduce (or indeed, eliminate) the potential for physical violence during the transaction. Second, by providing superior anonymity guarantying online anonymous marketplaces and participants shield from law enforcement intervention. Third, online anonymous marketplaces provide an escrow system to prevent financial risk. These systems are very similar to those developed by electronic commerce platforms such as eBay or the Amazon Marketplace. For example, suppose Alicia wants to purchase an item from Ted. Instead of directly paying Ted, she pays the marketplace operator, Oscar who then instructs Ted that he has received the payment and the item should be shipped. After Alicia confirms receipt of the item, Oscar releases the money held in escrow to Ted. This allows the marketplace to adjudicate any dispute that could arise if Ted claims the item has been shipped, but Alice claims not to have received it. Some marketplaces claim to support Bitcoin's recently standardized "multisig" feature which allows a transaction to be redeemed if, e.g., two out of three parties agree on its validity. For instance, Alicia and Ted could agree the funds be transferred without Oscar's explicit OK, which prevents the escrow funds from being lost if the marketplace is seized or Oscar is incapacitated.

Figure 8. Silk road system



Darknet Marketplaces

AlphaBay Market was operating on the Tor network. AlphaBay Market is owned by alpha02 and DeSnake, launched in December 2014. This market was said to be one of the largest Darknet Market tiers around the world. It had 2,40,000 active users on the internet and is devoted to the sale of both legal and non-legal items (i.e. illicit drugs, firearms). Alphabay seized by law enforcement, along with Hansa market.

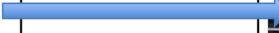
Dream Market is one of the best Escrow Darknet Marketplace and is established in the year 2013. In Dream Market, you can buy and sell goods from several vendors available on the market. It is a place for buying legal and illegal drug items. Dream Market satisfies both the drugs as well as digital assets. Dream Market drugs have a simple user interface (UI) and high administrative competence

Valhalla Market is a MultiSig or Trusted Invite Darknet Markets. They offer both traditional Escrow and Multisig, 2FA and Forced PGP. Valhalla (Silkkitie) Market recently turned to invite only and require a referral link to register as a buyer or vendor. They were rebranded and now called “Valhalla”. Valhalla Marketplace was established in the year October 2013 as Silkkitie. They started it as a local market for Finland and later became the largest international market ever so far. Silkkitie Market is one of the longest running markets on the Dark Web.

Opioid Sales and the Dark Web

A verification and monitoring service for online pharmacies name **Legit Script** collected data on top dark web drug marketplaces in 2016. A report was prepared for **CSIP** on the state of the internet pharmacy market, including market trends, challenges, and opportunities. The report revealed that approximately 96 percent of websites marketing pharmaceuticals on the open internet — somewhere between 30,000

Table 2. The darknet and drugs

Buyer places orders with the market	Buyer 	Market 	Vendor
Buyer sends Bitcoin to market escrow			
The vendor gets order & escrow confirmation			
Vendor ships product			
Buyer confirms Receipt			
Market releases escrow to the vendor			
Buyer leaves feedback on Market			

and 35,000 — failed to adhere to applicable legal requirements. Of those, the vast majority (all but about five percent) was blatantly illegal and unsafe, selling prescription drugs without requiring a prescription.

The report also revealed that the voluntary efforts of internet and payment platforms such as Google, PayPal, and Bing, among other companies, to curb the online promotion of illicit products have disrupted these illicit businesses' operations, specifically by removing the options of paid advertising and the most common payment methods

Illicit pharmaceutical dealers rely on search engine optimization (SEO) and third-party platforms in lieu of paid advertising. Drug vendors also take advantage of anonymous chat forums to find customers, but the most popular of, reddit.com, has recently seen more scrutiny and enforcement by platform operators.

The surface web is the battleground of an ongoing struggle between drug vendors looking for outlets to market their wares and those trying to stop them, which makes it more difficult for rogue internet pharmacies to maintain a stable presence on the surface web.

LegitScript compiled a list of about 240 marketplaces selling drugs on the dark web, and focused on 12 top marketplaces that sold drugs, including opioids, and were generally online during their research. From these marketplaces they collected data by hand, counting the number of drug listings, the types of drugs sold, the number of vendors for certain opioid products, and the locations from which vendors state they are shipping. Their data and analysis indicate that dark web commerce is concentrated in a handful marketplace and that one, in particular, Dream Market, currently dominates dark web drug commerce.

The anonymity of the dark web makes it ripe for scams, which is why vendor reputation is another pillar of dark web commerce. Customers leave vendor reviews in the same way they might on clear web e-commerce websites such as Amazon or eBay. However, reputation scores take on additional relevance because there is little recourse in the event of fraud. A verification and monitoring service for online pharmacies collected data on top dark web drug marketplaces,

The largest known exit scam is Evolution marketplace, which was abruptly shut down in 2015 and whose operators absconded with \$15 million worth of Bitcoins.

When Alpha bay, the dominant marketplace at the time, was shut down by law enforcement in July 2017, there was wide speculation that its operators had engaged in what would have been a massive exit scam. Some surface web websites track and review dark web marketplaces, rating them by factors such as whether they have had security issues or active warnings, whether they offer security technology such as multisig and two-factor authentication, and whether they have proven reliable and trustworthy.

Heroin comprised 2,294 or 54.6 percent of the opiate listings on Dream Market. The largest subcategories, oxycodone, and fentanyl comprised 11.4 percent and 5.5 percent, respectively. Nine of the 12 marketplaces surveyed broke opioids into subcategories. Of these, heroin was the most prevalent opiate listing in seven. Oxycodone was the second most prevalent opiate listing in four of these nine marketplaces and was first in one.

Prescription drugs on Dream Market are divided into only two subcategories: relaxants and stimulants. Of 2,468 prescription drug listings, 837 (33.9 percent) were classified as stimulants and 213 (8.6 percent) were classified as relaxants. Those not sub-classified fell into neither category, such as erectile dysfunction drugs.

Illicit e-commerce frequently draws vendors who engage in nondelivery schemes, in which sellers receive payment for products they never send. Although this appears to be less of a problem than on the surface web, nondelivery can still occur on the dark web, particularly from vendors targeting inexperienced buyers and from scammers Collaborating with operators of the marketplaces themselves.

Figure 9. Product statistics

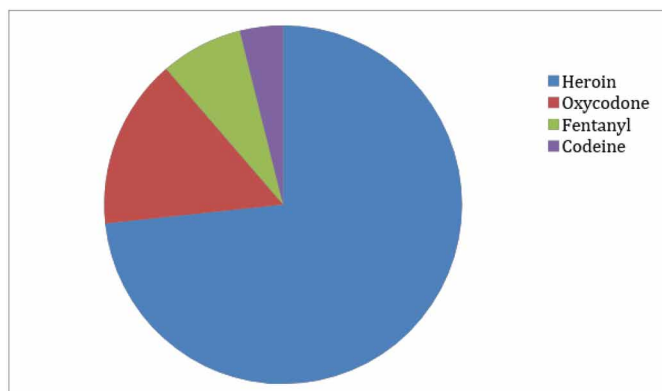


Table 3. The 12 dark web marketplaces surveyed by Legitscript

Marketplace	Primary .onion Address	Drug Listings	Opiate Listings
Dream Market	http://lchudifyeqm4ldjj.onion	58,382	4,204
Valhalla	http://valhallaxmn3fydu.onion	13,176	1,008
Tochka	http://tochka3evlj3sxdv.onion	8,934	1,691
Berlusconi Market	http://hky3mzk3jtm4zt4.onion	6,389	244
Wall Street Market	http://wallstyizjhkrvmj.onion	3,934	338
Olympus Market	http://olyymm2ravxnnf2hm.onion	2,988	139
Zion Market	http://zionshopusn6nopy.onion	2,546	173
Drug Market	http://4yjes6zfucnh7vcj.onion	2,303	83
Empire Market	http://libbyxh6som2twgp.onion	1,836	71
Empire Market	http://empiremktxgiovhm.onion	1,748	209
Silk Road 3	http://silkroad7rn2puhj.onion	~1,700	~233
Apollon Market	http://apollionih4ocqyd.onion	149	1
	Total	104,085	8,394

Table 4. Top fentanyl vendors on dream market by number of listings

Vendor Username	Fentanyl Listings	Alleged to Ship	Successful Transactions	Customer Rating (out of 5)
cdnven	45	Canada	1,400	4.88
HappyDrugs	29	EU	1550	4.86
mafision	24	Slavakia	80	4.69
The-Wired	19	China	480	4.80
TheDarkHorse	16	Hong Kong	210	4.72

DARK WEB AND THE CARDING ECOSYSTEM

The internet is ripe with stories about travelers who ‘hacked’ their way into cheap travel and vacation costs. In the cybercriminal underground, fraudulent online transactions involving travel documents, airline and hotel loyalty accounts, and other travel-related services have become valued commodities in the past several years. Cybercriminals run this business by offering services paid for using stolen credit cards, hacked loyalty program accounts that were either leaked or vulnerable, and fraudulent redemption of freebies, discounts, and rebates in the form of coupons, among others. Although there are existing security mechanisms in place to combat such illicit activities, cybercriminals continue to offer more and more services in hopes of piquing buyer interest.

The dark web, underground forums, Telegram channels, and even social network postings advertise these services with the intention of providing cheap price tags for those who do not have a problem breaking the law. From arranged travel documents and car rentals to booking flights and hotel rooms, some of the services are offered in the Chinese and Russian underground and some English-language forums:

Digital Shadows' intelligence analysts have identified a Telegram Market gaining traction called "OLIMP". OLIMP has been active since August 2017 looks to provide a new format for buying and selling these goods and services. This is all made easy by the creation of a bot to automate the browsing of these shops. There is a range of items for sale on OLIMP, including discounted hotels, drugs, taxis, documents, and driving licenses. OLIMP has a wide range of items for sale including discounted hotels, drugs, taxis, driver's licenses and documents. For example, the latter offering includes counterfeit press passes for events.

The Dark Web Drawbacks

Because the content on the dark web (often called "hidden services") is not indexed by traditional search engines, and because there is no registration of domain names overseen by a single entity such as the Internet Corporation for Assigned Names and Numbers (ICANN), it's impossible to give a specific, accurate snapshot of content and traffic. Indeed, this is part of what makes the dark web "dark." Hidden services on the dark web are also notoriously slow and unreliable, frequently cycling online and offline multiple times in the same week, or even the same day. A primary reason for this instability is that the dark web is highly decentralized, relying on networks of private servers, which may be something as simple as a person's old laptop. As a result of the way, Tor software works — routing users through multiple relays —the experience of navigating hidden services can be painfully slow.

Tor Metrics collects anonymized data on user's services, and traffic operating through Tor software.

Between April 2017 and March 2018, the number of .onion address ranged from about 45,000 to about 72,000. March 2018, the number was about 68,000. This number does not equate to actual websites on the dark web because hidden services often have multiple .onion addresses. (For example, the dark web marketplace Dream The market has 11 .onion addresses.) Many of these websites may also have no content. In early 2015, Tor Metrics estimated that there were about 30,000 hidden services. The volatility makes it difficult to tell if there is a trend upward. In 2016, .onion Addresses spiked to 114,000. Kate Krauss, Director of Communications and Public Policy for the Tor Project stated that "it's not difficult for even one person—a Researcher, for instance—to create a lot of new onion addresses—which is not the same as actual websites or services. Tor Metrics estimated daily usage of anywhere from about 2 million to close to 5 million.

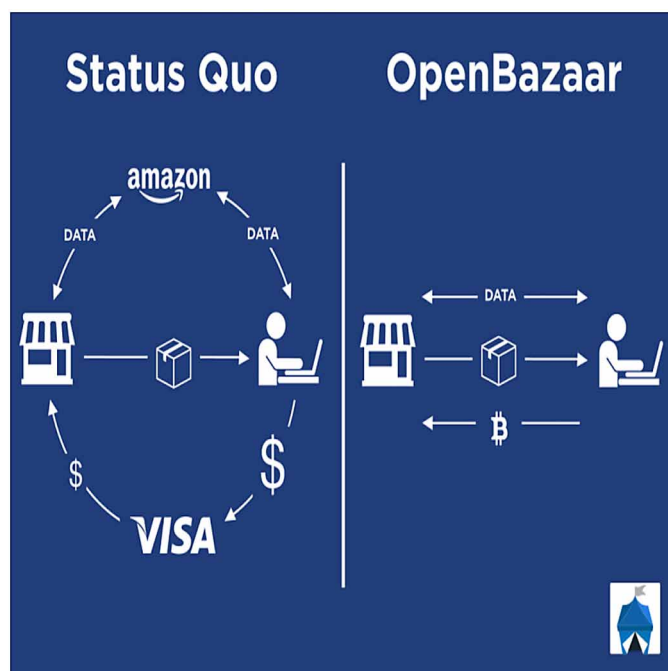
Dark Web Alternatives

Another weakness of Dark Web marketplaces is their dependence on an operator, or group of operators, who control the sites. Once they're spotted, these persons can be tracked down and prosecuted. The development of decentralized marketplaces such as OpenBazaar generates new challenges that do not exist with Dark Web markets. With OpenBazaar, there is no marketplace operator for law enforcement to target. On the other hand, each individual user engaged in illicit commerce could become a target instead. Decentralized markets are also much harder to shut down.

Since the launch of OpenBazaar 2.0 in late 2017, the network has seen over 100k nodes created and 20k nodes with at least one listing. "Nodes" means the installation of the app and creation of a profile or store that can connect to others on the network and be discovered. OpenBazaar is still in its infancy.

The platform does not anonymize the user by default. Originally, it was entirely on the user to mask their identity if they desired. Now, since the release of OpenBazaar 2.0, users can opt to access the site using a Tor browser, which allows great anonymity. Payments can be made using Bitcoin, but you also have the option to pay using traditional formats.

Figure 10. Open bazaar



Most of the items sold on OpenBazaar are simple consumer goods. On OpenBazaar, you can find items such as food, cigarettes, clothing, and accessories. OpenBazaar is a neutral technology that can be used for many types of transactions. It was not created to cater to any particular type of commerce, such as illicit and illegal goods. Like any technology, much like the Internet itself, the OpenBazaar network reflects society in general: some people will do bad things, most will not.

To locate products on OpenBazaar, you must select a search engine and each search engine will list different products. According to tests, when searching using the OB1 engine, no drugs were found. However, when switching to the Blocktooth engine, a number of cannabis products and other drug-related items were listed. By using different search providers or if you know the vendor's URL, you may be able to access an even wider array of illicit goods. It's impossible to know. Even OpenBazaar has no insight into what is being sold on its platform, and in what numbers.

Counterfeit and stolen merchandise could find a home on OpenBazaar, providing sellers with a level of anonymity that parallels the Dark Web, but using a platform with enough mainstream appeal to increase visibility and reach on the Surface Web over time. Selling counterfeit or stolen goods is possible through OpenBazaar, and if there is such an opportunity there will be those who will want to exploit it.

While the Dark Web and OpenBazaar function in different ways, the outcomes for the seller are quite similar. On OpenBazaar, anyone can sell anything they want. They can mask their identity and hide their location. It is on the side of the user that the real benefits are clear, in that it is much more difficult to scam users in the way that is done on the Dark Web. This can only help the OpenBazaar platform as it establishes itself and evolves to become a viable alternative to the Dark Web. For security professionals, the problem of combating illicit trade continues to become more complex and the number of online locations to monitor more daunting.

Peer-to-peer services such as OpenBazaar remove the middleman and allow illicit operations the best of both worlds: the privacy of the dark web on easily accessible and navigable software. Users can still obfuscate their identities using a VPN. Other decentralized marketplaces include Particle, SysCoin, and BitBay. All of these are powered by blockchain and offer encrypted peer-to-peer messaging for privacy.

Combatting the Dark Web with Technology

On December 6 and 7, 2017, the US Department of Health and Human Services (HHS) hosted its first Code-a-Thon event aimed at leveraging technology and data-driven solutions to help combat the opioid epidemic. The authors—an interdisciplinary team from academia, the private sector, and the US Centers for Disease Control and Prevention—participated in the Code-a-Thon as part of the prevention track.

Objective

The aim of this study was to develop and deploy a methodology using machine learning to accurately detect the marketing and sale of opioids by illicit online sellers via Twitter as part of participation at the HHS Opioid Code-a-Thon event.

Methods

Tweets were collected from the Twitter public application programming interface stream filtered for common prescription opioid keywords in conjunction with participation in the Code-a-Thon from November 15, 2017, to December 5, 2017. An unsupervised machine learning–based approach was developed and used during the Code-a-Thon competition (24 hours) to obtain a summary of the content of the tweets to isolate those clusters associated with illegal online marketing and sale using a bi-term topic model (BTM). After isolating relevant tweets, hyperlinks associated with these tweets were reviewed to assess the characteristics of illegal online sellers.

Results

Researchers collected and analyzed 213,041 tweets over the course of the Code-a-Thon containing keywords codeine, Percocet, Vicodin, Oxycontin, oxycodone, fentanyl, and hydrocodone. Using BTM, 0.32% (692/213,041) tweets were identified as being associated with illegal online marketing and sale of prescription opioids. After removing duplicates and dead links, we identified 34 unique “live” tweets, with 44% (15/34) directing consumers to illicit online pharmacies, 32% (11/34) linked to individual drug sellers, and 21% (7/34) used by marketing affiliates. In addition to offering the “no prescription” sale of opioids, many of these vendors also sold other controlled substances and illicit drugs.

The results of this study are in line with prior studies that have identified social media platforms, including Twitter, as a potential conduit for supply and sale of illicit opioids. To translate these results into action, authors also developed a prototype wireframe for the purposes of detecting, classifying, and reporting illicit online pharmacy tweets selling controlled substances illegally to the US Food and Drug Administration and the US Drug Enforcement Agency. Further development of solutions based on these methods has the potential to proactively alert regulators and law enforcement agencies of illegal opioid sales, while also making the online environment safer for the public.

FUTURE RESEARCH DIRECTIONS AND TRENDS

The anonymity and cryptographic approaches used by dark web visitors impose serious challenges for law enforcement agencies to monitor, investigate, control, and prosecute criminal activities taking part in these darker parts of the internet. Digital Forensics offers methods and tools for identification, collection, analysis, and reporting of information obtained from the dark web in a forensically sound way.

Computer Forensics and Cybercrime Investigation is a fairly new area of research among the more conventional computer security models, there are currently some companies and open-source communities that specialize in forensic investigations. The following represent the most commonly used tools during evidence collection of a digital investigation:

1. **Firewall and Router Logs:** These devices are configured so that they may record any form of suspicious activity.
2. **Packet Sniffing:** This procedure enables the investigator to monitor in real time various activities taking place on a network.
3. **Intrusion Detection Systems (IDS):** Larger networks can sometimes deploy IDS to capture data packets that can be linked to suspicious activities.
4. **Remote Access Servers:** This includes devices, e.g. modem servers and VPN gateways, that facilitate various forms of connections between networks.
5. **Security Event Management Software:** These tools help with the analysis of log files which are typically produced by IDS tools, routers, and firewalls.
6. **Network Forensic Analysis Tools:** These tools are useful in reconstructing events via visualization and replaying of network traffic taking place within a given period of time.
7. **Other Sources:** These sources can include Internet Service Provider (ISP) records, hosts' network connections, and configuration, client/server applications, and Dynamic Host Configuration Protocol (DHCP) record.

Artificial Intelligence and Machine Learning

Machine learning algorithms can help police sweep the dark web and crack down on cybercrime. But beyond evidence of illegal activity, it's helping law enforcement find something far more valuable: motive.

A recent study was conducted with permission from the Australian Federal Police (AFP), by Monash University IT researchers. They conducted an extensive crawl of the dark web to test a classification model named Tor-use Motivation Model (TMM), used to capture user behavior and motivation that can be applied in law enforcement.

Monash University

For legal and ethical considerations, AFP federal agent and Monash Ph.D. candidate Janis Dalins led the research. He emphasized the value of the two organizations working together. In particular, they hoped to draw out not just what kind of material the sites were hosting, but why.

With permission from the federal justice minister, the researchers developed a randomized web crawler that used Tor to access more than 232,000 anonymous pages. Dalins manually classified more than 4000 of these pages according to content and use.

The researchers tested a motivation model using The Onion Router, (TOR), to crawl through thousands of pages of content to classify what it is used for, and how much of it is illegal.

The unrestricted crawl of 200,000 sites showed that two-thirds were illegal and unethical. Of the illegal sites identified, the majority were devoted to the financial activity, such as bitcoin laundering. Other illegal sites included those related to drug commerce and trading of illicit materials such as child pornography.

Nearly 40 percent of the pages analyzed were legitimate. When added to content that was unclear in its intent, it's likely that over half of the material analyzed would not be of interest to law enforcement officials.

Of the illegal material, the most frequently encountered category was a financial crime, at 16 percent of the pages accessed. Of these sites, 95 percent offered products and services for sale, including bitcoin laundering sites and exchanges. Stolen credit cards, bank account details, and gift cards were also on offer.

The follow-up study will focus on applying the classification system to train machine learning algorithms that could be used by police to weed out crime on the dark web and other online platforms in the future.

The results of the study, published in *Digital Investigation*, has shed some light on the dark web highlighting the use of advanced technology giving law enforcement agencies new tools to find - and fight - illegal activity online.

Medical Big Data

Medical Big Data is currently being offered for sale on the dark web. Medical big data relies on medical documentation representing one of the most comprehensive means for collection of information regarding a person's identity, and other personal sensitive private information. The first large-scale theft was recorded by the US Department of Health and Human Services in 2012. In subsequent years, there were more thefts on a similar scale, reaching around a thousand by 2016. In particular, the attention of hackers focused on the theft of personal data, date of birth, addresses of patients, and in particular social security numbers.

Medical information can be worth 10 times more than credit card numbers that are offered for sale on darknet marketplaces. Those who are willing to buy this type of information are mainly fraudsters who can easily use this data to create fake IDs, to buy medical equipment with reimbursement, or even drugs.

Cocaine Delivered Quicker Than Pizza

Professor Adam R Winstock, a consultant psychiatrist and founder of Global Drug Survey, conducted a survey and asked 15,000 cocaine users from around the world whether it was quicker to get a gram of cocaine delivered or a pizza. Overall 30% said they could get cocaine delivered in 30 minutes or less compared to only 16.5% who could get a pizza delivered. There was wide regional variation but in the UK, 80% of recent users reported same day delivery of cocaine being available, with 36.7% of users in Glasgow and 26.7% in London reporting delivery within 30 minutes. Easy access and higher purity are likely to lead to escalating use and harm among people.

Survey findings also revealed that the UK once again had the highest rates (24.6%) of people accessing drugs through the darknet amongst English speaking countries and 3rd overall after Norway (30.3%) and Finland (45.8%). MDMA, followed by cannabis, LSD and novel drugs are the most commonly purchased drugs on the darknet, with notable increases in rates for cannabis and LSD over the last 4 years, with a marching year on year decline in NPS purchase.

SOLUTIONS AND RECOMMENDATIONS

The Dutch law enforcement unit mandated to fight cyber-crime has recruited 14 volunteers comprised of IT experts in order to strengthen the fight against dark web crime. International police organizations like Europol and Interpol are taking dark web crimes very seriously, whereby, in the recent meeting held in Dubai, among the issues discussed was dark web crime. Dutch law enforcement has been at the forefront of the fight against dark web illegal activities. The Dutch detectives were responsible for Operation Bayonet, which took down a popular dark web marketplace known as Hansa.

Existing laws along with the mindset of law enforcement agencies need to evolve to confront the challenges of potential cybercrimes in 2020. In addition, law-enforcement agencies need to upgrade themselves with the latest technologies such as artificial intelligence and robotics to better tackle future cybercrime. Internet protocol (IP) address or source tracing remains a challenge due to the use of proxies, virtual private networks (VPNs) or Tor relay points. A possible solution to this might be an allocation of IPv6 addresses on an individual basis. If every user is allocated an IPv6 address, which is required to connect to the internet, it will eliminate the issue of IP tracing. A combination of increased user awareness and use of advanced technologies for defense will go a long way in helping individuals and enforcement agencies deal with the future of cybercrime.

Rather than shaping technology to conform to international law based on national sovereignty, countries can find new ways of enforcing existing laws. For example, cooperation on investigations of cross-border data flows would allow law enforcement to respond to threats more quickly.

Countries might exercise sovereignty rights for setting their specific rules with respect to when data should be stored and processed by different authorities for reliable and legitimate purposes. It is important for authorities to be on their toes in safeguarding the same from future unknown hacking techniques.

CONCLUSION

November 1, 2017, Finnish Customs in collaboration with the police shut down the Sipulikanava website. This marked the biggest ever shut down in the country. The accused are two Finnish nationals and one a 45-year-old IT wizard who also was the Sipulikanava website's administrator. This case also marks the first time, the administrator of a dark web marketplace is being accused of dealing large quantities of narcotics online.

With advancements in digitization and organizations, individuals, as well as defense establishments, would be potential targets of cybercriminal activities. The rise of cybercrime in the current year serves as a great signal for the incrementing societal engagement in issues of data protection and internet governance. It is assumed that citizens will demand greater transparency as well as accountability from the governments and service providers, and even some kind of data autonomy. Taking a cue from Europe's General Data Protection Regulation (GDPR), it is important for governments and businesses to understand that an individual's data is his or her asset and eventually individual's rights can be exercised under a mature regulated environment. Therefore it is important for increased data protection and governance culture. As new technologies like the internet of things continue to evolve, the ability of international law to combat their negative uses becomes increasingly important.

REFERENCES

- Albanese, J. S. (2011). *Albanese Jay S, Transnational Crime and the 21st Century Criminal Enterprise, Corruption, and Opportunity*. Oxford University Press.
- Alderman, K. (2012). Honor Amongst Thieves: Crime and the Illicit Antiquities Trade. *Honor Amongst Thieves: Crime and the Illicit Antiquities Trade*, 45(3), 602-627. Retrieved October 30, 2018, from <http://journals.iupui.edu/index.php/inlawrev/article/view/18002/18120>
- Barrett, M. J., & Ferris, J. A. (2014). *Use of Silk Road, the online drug marketplace, in the United Kingdom* (5th ed., Vol. 109). Australia and the United States: Society for the Study of Addiction; doi:10.1111/add.12470
- Cole, G. F., Smith, C. E., & DeJong, C. (2018). *The American System Of Criminal Justice* (16th ed.). Boston, MA: Cengage.
- Dalins, J., Wilson, C., & Carman, M. (2017). Criminal motivation on the dark web: A categorization model for law enforcement. *Digital Investigation*, 24, 62–71. doi:10.1016/j.diin.2017.12.003
- Crime, E. T. O. C. (2011). Why Lawyers Need To Understand It. *Pittsburg Journal of Technology Law & Policy*, 11(4), 1-54. Retrieved November 3, 2018, from <https://tlp.law.pitt.edu/ojs/index.php/tlp/article/download/62/62>
- Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. (2015). *International Journal of Drug Policy*, 26(11), 1113-1123. doi:10.1016/j.drugpo.2015.01.008
- Greenberg, A. (2013, November 8). Meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins. *Forbes*. Retrieved from <https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#637eb51f3d9b>
- Katelyn, G., & Holtfreter, K. (2017). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims & Offenders*, 12(5), 741–760. doi:10.1080/15564886.2016.1177766
- Mackey, T., Kalyanam, J., & Kuzmenzo, E. (2018). Solution to Detect, Classify, and Report Illicit Online Marketing and Sales of Controlled Substances via Twitter: Using Machine Learning and Web Forensics to Combat Digital Opioid Access. *Journal of Medical Internet Research*, 20(4), e10029. <https://www.jmir.org/2018/4/e10029/pdf> doi:10.2196/10029 PubMed
- Marta & Modrzewski. (n.d.). Darknet and Medical Big Data. Deep Internet as a Space for Illegal Trade in Medical Information. Retrieved from <http://www.atut.ig.pl/files/big-data.pdf#page=49>
- Popvov, O., Bergman, J., & Valassi, C. (2018, November 15). A Framework for a Forensically Sound Harvesting the Dark Web. *Proceedings of the Central European Cybersecurity Conference*.
- Segal, L., Ngugi, B., & Mana, J. (2011). Credit Card Fraud: A New Perspective On Tackling An Intransigent Problem. *Fordham Journal of Corporate & Financial Law*, 16(4), 743-781. Retrieved October 20, 2018, <https://ir.lawnet.fordham.edu/jcfl/vol16/iss4/2>

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In Proceedings of the 24th USENIX Security Symposium. Washington, DC: USENIX. Retrieved from <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf>

The State of Opioid Sales on the Dark Web. (2016). Prepared by LegitScript for The Center for Safe Internet Pharmacies (pp. 1-47, Rep.). Retrieved from <https://safemedsonline.org/wp-content/uploads/2018/06/Opioid-Sales-on-the-Dark-Web-LegitScript-June-2018-Report.pdf>

Updated: List of Dark Net Markets (Tor & I2P). (2018, October 15). Retrieved November 3, 2013, from <https://www.deepdotweb.com/2013/10/28/updated-list-of-hidden-marketplaces-tor-i2p/>

The Dark Web: Hidden Access to Internet Today

1

Ramanujam Elangovan

 <https://orcid.org/0000-0003-1450-9097>

Thiagarajar College of Engineering, India

INTRODUCTION

Internet is a hardware asset consists of multiple nodes where each node is a server/ client systems such as laptops, computers, etc. In earlier days, the data are transferred or shared using the Internet. In 1994, Berners-Lee et al introduced web in which the data are accessed through hyperlink text or web pages. Web is software which runs over the internet to provide the service to users. Only 4-6% of the whole web or the web pages (surface web) are indexed in search engines such as Google, yahoo, etc. However, web which is not indexed in search engines is 400 times larger than surface web also known as deep web. The deep web (Bergman, 2001) can only be accessed through a special link or with special permission to access the data in the cloud or specialized servers which cannot be found on any of search engines. Government sectors, private bank data, cloud data, etc are examples of the deep web. The data in the deep web are so sensitive and private which are to be kept in secret. These data are allowed to access only by specific people. There is a subset of deep web termed as dark web (Chen et al, 2008). Figure 1 shows the difference of Surface web, Deep web and Dark web.

Dark web allows a user to host a website on a specific network termed as dark net which remains anonymous always. The network used by the user to maintain anonymity is dark net. Dark net is a network build over the internet which is completely encrypted. Traditionally, when a user visits any sites,

Figure 1. Difference of surface web, deep web and dark web

Source: LeMacnalle



DOI: 10.4018/978-1-5225-9715-5.ch008

they are tracked via their Internet Protocol (IP) address. However, the dark net maintains privacy through specialized anonymity software and configurations to access. One such dark net is Tor (“The Onion Routing” project) (Dingledine et al, 2004).

TOR AND DARK WEB

The TOR architecture provides two basic services – anonymous browsing and hosting of anonymous information exchanges. These services are provided by one piece of special software – ‘Tor Browser’. There is no special technical requirement for these services to be bundled. Indeed, browsing is more popular than hosting. No Tor users have visited any hidden website at a *.onion address. Most probably, all the users merely use Tor browser to browse the internet’s conventional address space more securely. For example, Mary, who lives in a small town, wants to buy a pregnancy test but doesn’t want to be seen doing so by the shop owner. Peter, a friend of Mary’s father, wears a mask, walks detours and pay in cash. Peter will not be able to identify or trace. Also, Mary’s privacy and anonymity are assured. Anonymous browsing is not actually a part of ‘dark web’, but it is a legitimate and impressive service provided by Tor. The underlying purpose was to create a distributed, anonymous easily deployable and encrypted network to be used by those who needed it. Specifically, it was offered as a free service to promote unfettered access to the internet in locations where online censorship was heavily enforced. Chaum in 2003 provided a way for this access through onion routing. In order for a user to access the website securely, the person has to be routed through a series of intermediary servers. The resulting pathways between servers were labeled ‘circuits’. Each packet of information to be relayed over the network would be encased in multiple layers of encryption, each to be sequentially peeled away only by the subsequent node in the circuit. Consequently, intermediary nodes could only decrypt one layer of the encryption, preventing access to the underlying data and its originator. The final such hop – or exit node – would reveal the original packet and proceed to deliver it to the desired destination, thus protecting the sender’s identity. As a result, intercepting and decoding the information along its path would be significantly harder – albeit not impossible – to accomplish. The dark web attracted the people who do illegal stuff such as trade, forums, media exchange for terrorists, etc. without getting caught. “Silk Road” is a dark web site which is used to sell drugs and was taken down already by FBI (Cubrilovic, 2014). Friend-Friend and Free net is also a dark web provided by darknet used to transfer file anonymously.

THE SIZE OF THE DARK WEB ECONOMY

The dark web, an ocean of illicit activity often carried out by persons to trade stolen data, dollars, etc. In 2016, the economist reported that usage of dark web by drug side grew from \$15 in 2012 to approximately \$225 million in 2019. On estimating the world economy, the dark web has frustrated every attempt of money and other information transactions. In the year 2023, the dark web cybercrime will be an increase of 175% increase as reported by Juniper research. Dark web is increasingly used by hackers like hire, hitmen and other service providers who can’t advertise over traditional channels. Also, the year 2017 has been recognized as the most notorious year for selling ransomware for Dark web. Even a casual news consumer can feel the ransomware attacks cost an estimated worldwide business of \$1 billion this

year. *Carbon Black's Threat Analysis Unit (TAU)* has investigated the deepest, darkest portion on the web, where ransomware is currently being created, bought and sold in rapidly increasing underground economies. The research has found that in the financial year 2018-2019 there has been 36.5% increase in the sale of ransomware on the dark web. The research found that, in the financial year 2016-2017, there has been a 25.2% increase in the sale of ransomware on the dark web. This large scale increase is due to supply and demand of the world's economy. Cybercriminals are progressively looking for more opportunities to enter the market and to make quick money via any one of the many ransomware offerings available via illicit economies. In addition, a basic plan of ransomware is its turnkey. Unlike other forms of cyberattacks, ransomware can be quickly deployed with a high probability of profit. The interesting information is, the dark web economies are also empowering even the most novice criminals to launch ransomware attacks via do-it-yourself kits and providing successful ransomware researchers with annual incomes into six figures.

KEY FINDINGS OF DARKWEB RANSOWARE

- Currently more than 63,000 dark web marketplaces are selling ransomware with 45,000 product listings. The prices for the do-it-yourself (DIY) kits range from \$0.50 to \$3K.
- Comparing to the year 2016 target, the ransomware marketplace of 2017 on the dark web has grown to a rate of 2,502%. According to the FBI, ransom payments totaled about \$1B in 2016, which was \$24M in 2015.
- According to figures from Payscale.com, ransomware sellers are making more than \$100,000 per year simply retailing ransomware, however, the legitimate developers earn only to a maximum of \$69000.
- The most notable innovations contributing to the success of dark web ransomware economy has been the emergence of Bitcoin for payment, Tor for anonymity network.
- Ransomware sellers are increasingly specializing in a specific area of the supply chain, further contributing to ransomware's boom and economy development.

REGULATING THE DARK WEB

To regulate the dark web, the regulators have struggled a lot with enforcement. In 2013, FBI has taken down Silk Road (Van Hout et al, 2013), a popular drug market of the dark web in 2013. Silk Road 2 popped up in 2014 before FBI has taken up Silk Road. Silk Road 3 followed of course. In addition to difficulty in stamping out new marketplaces, OpenBazaar has provided opensource code which allows for decentralized marketplaces similar to how torrents allow for decentralized file sharing. So, the dark web economy continues to grow despite the best efforts of law enforcement. A recent study from researchers at King's College London gives the following breakdown of content by an alternative category set, highlighting the illicit use of ".onion" services for the access of Dark webs. The objective of the proposed chapter is also to exploit the illegal access of Dark nets g, through webs and the benefited user through the webs. Also, this chapter explains about the actions taken by the National agencies like cybercrime and cybersecurity office (Manikandakumar et al, 2018) towards the Dark web.

ILLICIT USE OF “ONION” SERVICES

Botnets

Botnets (Barford et al, 2007) are one of the major threats faced by Internet users. Hackers mostly used botnets for many kinds of malicious activities or to spread malicious activities such as DDoS attacks, phishing attacks, personal data theft, spam, bitcoin mining, and cyber-espionage. Traditionally, botnets used centralized overlay networks where the Command-and-Control(C&C) acts as a single point of control. In case of failure, or taking down C&C servers, the whole botnet will be defeated. Hence, Botmasters have recently focused their attention to the Tor network to provide the botnet C&C servers with anonymity. The advantages of botnets over the Tor network may provide

- High availability and low downtime of authenticated hidden services
- Reasonable availability of private networks
- Debug node flooding capabilities.

The use of Tor network to hide botnet infrastructures evolved during 2010. Brown in 2010, has provided the first demonstration of C&C servers and its applications through Tor network to provide anonymity. Guarnieri, 2012 has first identified a mechanism to detect and analyze the first Tor-based botnet. The modified version of a botnet with Zeus enables the user to do illegal stuff such as bitcoin mining and credential thefts. The malware designed by any hacker with Zeus bot, Tor client, and few libraries for GPU crash any number of systems. Later in 2013, the Tor mailing list (Munson, 2013) raised the attention of hackers to use huge networks and users in real-time processing. Due to the enormous usage of Tor networks, computational overload caused the expensive encryption operations to have reduced the responsiveness of the system.

Bitcoin Services

Bitcoin (Nakamoto, 2008) uses a peer-to-peer technology (P2P digital currency) to operate with no central authority such as banks or under any Government agencies. Transactions and issuing of coins are managed by over collective of the distributed network. The anonymity is provided by random-looking Bitcoin addresses, however, the level of anonymity is very low as suggested in various research (Biryukov et al, 2015). This encourages the Bitcoin users to use the network through dark nets such as the Tor network. Dark web and the Bitcoin have a strong relationship, as Bitcoin is often used on the dark web. Most of the e-commerce sites on dark nets allow users to do any kind transactions to buy and sell goods using Bitcoin. The Silk Road (Vanhout et al, 2013) is one of the most famous darknet sites specialized in purchasing drugs with Bitcoin. All over the world, there are 12 Bitcoin related cases filed. Seven of them operate on Silk Road, which involves the owner of the Silk Road and his employees, drug vendors, and Bitcoin vendors operating on this site. Finally, two FBI agents were charged for money laundering and wire fraud. The vendor who needs to sell any drugs in Silk Road, they must be aware of the following. Initially, the vendor who needs to do any transaction on dark nets with Bitcoin must have enough knowledge of Tor service to access Silk Road. Second, they have to create a store on the Silk Road. As like e-commerce sites Amazon, Flipkart, Silk Road provides a system to rank the vendors base on the quality and frequent purchase by customers. It also allows the customer to leave a comment using a five-star rating system. The drug vendors Sadler and White did the online drug business for more

than one year and ranked no 1 among top sellers. Also, there were 142 customer feedback pages rating with mostly 5 stars. In addition to a ranking system to the customer, Silk Road launched a “4/20” scale a free paid trip to Thailand with a total cost of approximately \$30,000. The final step of any vendor is to acquire bitcoin and prepare an address for delivery. If buyers didn’t have any Bitcoins they can avail Bitcoin exchange service to change their fiat currency to any Bitcoin. The fourth step is the delivery and payment. To prevent controlled delivery, Silk Road provides detailed guidelines to help their customers from further investigations. To avoid from regular postal investigations with sniffer dogs, vendors used a vacuum-sealed and zip lock cover to seal the drugs. Silk Road uses a special system for payment. The buyers who purchased any drugs transfer their bitcoin through online once received by the vendors, they will deliver the products.

Crypto Markets

Crypto markets (Martin, 2014) are online commercial websites or marketplaces that are part of dark web operate via dark net such as Tor or I2P. The main objective of crypto markets is for the sale of illicit drugs, whole sale black markets, brokering transactions on drugs, cyber-arms, steroids. They provide tools for anonymity to the participants with the purchase and delivery of products through illicit drug trafficking. Following the Silk Road model, crypto markets are characterized by their usage of darknet anonymized access and bitcoin payment with escrow services. Canada was in Top 5 of the most frequent shipping on Silk Road, with 6% of the listing originated from Canada. The paper Broseus et al, 2016 reports, Agora, Silk Road2, and Evolution are three main crypto markets in terms of their number of vendors and customers active on them and products on sale. None of these crypto markets are currently running due to certain reasons (Gibbs, 2018). The Table 1 values are referred from Broséus et al, 2016. The Table 2 list the product often purchase through crypto markets and their break down ratio.

Hacking Groups and Services

The dark web is one of the most charming remnants of humanity, aggregated marsh of all the darkest aspects of internet activity such as child abuse images (kiss, 2013), drug markets, gun shops, gore smut, stolen merchandise, anarchist guides, terrorist chats, identity theft, hacking services and even more. The following describes about the potent of using these services for hacking (Marin et al, 2016). The

Table 1. Number of vendors and listings originating from Canada

Crypto markets	Number of Vendors	Number of listings
Agora	57	1109
Evolution	44	691
Silk Road 2	36	748
Cloud Nine	27	395
Pandora	18	398
Hydra	8	79
Andromeda	5	149
Blue sky	3	116
Total	198	3685

Table 2. Vendor product breakdown as on 3 June 2016

S.No	Product	Breakdown (%)
1	Cannabis	31.6
2	Pharmaceuticals	21.05
3	3,4-Methylene Dioxy Methamphet Amine (MDMA)	10.530
4	Lysergic acid diethylamide (LSD)	5.26
5	Methamphetamine	5.26
6	Mushrooms	5.26
7	Heroin	5.26
8	Seeds	5.26
9	Video Games	5.26
10	Accounts	5.26

user what actually think is “Browsing porn in incognito mode isn’t nearly as private as you think”. One of the largest hacking forums on the internet which uses the concept of Dark web is FreeHacks. It’s a Russian community which aims to collectively gather its resources in order to maximize efficiency and knowledge dispersement. It works similar to any typical forum, as like opening the Tor browser, copy and paste the URL, and land on a home page with various sub-forums. The sub forums are of varied and well divide into different categories as like

- Hacker world news
- Humor
- Hacking and security
- Carding (stealing credit cards and trying to cash them out on the internet)
- Botnet (a network of bots used to steal data and send spam, or perform DDOS attacks)
- Electronics and phreaking (phreaking is trying to break someone’s security network)
- Brutus (software used to crack passwords)
- DDOS (overwhelming a server with requests to shut it down)
- SEO-optimization
- Programming
- Web development
- Malware and exploits
- Private software
- Clothing market (people who use stolen credit cards to buy clothes and resell them)
- Financial operations
- Documentation (passports, driving licenses, citizenships)
- Blacklist (a community judicial system).

The above mentioned illegal activity covers a dizzying amount of information, from a Russian forum and has more than about 5,000 active members. This is just the overview; even every sub-forum is further splitted into dozens of other sub-forums. When a user attempts to register on any hacking site, you’re met with a mission statement of sorts – a weird justification method for their own illegal activities. Once you

go through the rigorous registration process where you have to declare why you want to join the forum, and what software development skills you have and want to learn, you are granted access to this treasure trove of illicit information. It seems more pathological and ironic; these hackers who essentially get paid to make life more difficult for people try to justify it with a fascinating proclamation.

The word 'hacker' is incorrectly used in the meaning of 'computer burglar' by some journalists. However, hackers, refuse to accept such an interpretation of it and continue to imply the meaning of 'someone who likes to program and enjoy it'

FRAUD SERVICES

In recent days, more number of fraudulent services (Moore et al, 2016) has emerged such as falsification of documents, forgery or counterfeit are types of fraud. The theft of one's personal information, like social security number or identity is type of fraud. Fraud can be communicated through many media includes mail, wire, phone and the internet may be computer fraud and internet fraud. However, in dark web, fraudulent refund services are now becoming another fierce of attack for malicious actors (Alrwais et al, 2014). The malicious actors' targets online retailers, banking sectors on their generous refund policies to fraudulently claim money or replacements for products they hadn't purchased. These services are particularly persistent form of a cybercrime since merchants are stuck between trying to ensure customer satisfaction and mitigating the loss of an estimated 50,000 Euros every month through cybercrime. For an example, a typical fraud case occurs when the false buyer claims that the product they allegedly purchased has never arrived. Due to the severe competition going on between online retailers, many of them promptly respond to such claims with the refunds or replacements purely to control damage to their reputation and to keep the customer happy.

Refund fraudulent services have grown significantly since 2017, coasting on the increasing number of online sales. Refund services are openly discussed on the dark web forums where fraudulent vendors are quick to offer their "specialized services" to the interested third parties. In return for effective service, these illegal vendors gain enormous followings and create a reputation that is conducive to the continuity of their business. Happy customers have been known to go as far as leaving screenshots alongside messages of gratitude and praise following a successful refund scam. Vendors who pull off scam after scam successfully will often receive repeat business from many of their customers, who are sometimes satisfied enough to leave positive reviews about their experience. Even as online retailers struggle to figure out a way around this scam, more and more illicit vendors pop up on these dark web forums offering their services.

This kind of increase in criminal activity has led to an invasion in the advertisement of fraudulent receipts on the dark web. These fake receipts (Baravalle et al, 2016) often look as authentic as the next and can be engineered to target a wide variety of online retailers. Fake receipt vendors rely on social engineering as their main approach since there are no parameters to be bypassed in this scenario. The customizable nature of these fake receipts only makes it more difficult for companies to preempt these actors next move. These receipts also present a huge problem for many online stores as Flashpoint analysts cautiously predict. In addition to saturating the market with an indeterminate number of fake receipts, these illicit vendors have made it easier for malicious actors to claim reimbursement even without making the initial purchase. Similarly, they have made it increasingly difficult for companies to spot instances of fraud even if they're perpetrated by the same person.

The availability of physical fake receipts will make it harder for stores to suspend people from using them to wrongfully claim reimbursement. As an added risk, the physical receipts will make it impossible for the retailers to avoid reimbursing customers for stolen products. Several illicit vendors offer digital and virtual receipts alongside product serial numbers just to increase the legitimacy of the claim. Aside from the very pertinent concern of having a market that is flooded with fake serial numbers, the availability of fake product serial numbers leads Flashpoint analysts to speculate that these vendors are in possession of the serial number-generating software. Already, several of these types of software have been spotted on various forums both on the dark web and on the surface web.

Increase in the competition between the online retailers and a need for transparency will continue to force retailers to extend munificent policies, usually at their own expense. This gap is one that may only widen a business's compete to differentiate themselves and to build loyal customer bases. As miserable as the situation appears to be, online businesses can avoid falling for some of these fraudulent claims by carefully analyzing all refund claims before fulfilling them. A dedicated intelligence service can facilitate this and help businesses to avoid massive losses from cybercrime.

Hoaxes and Unverified Content

An assassination market (Moore et al, 2016) is a prediction market where any party can place a bet (using anonymous electronic money and pseudonymous remailers) on the date of death of a given individual, and collect a payoff if they “guess” the date accurately. This would incentivize assassination of individuals because the assassin, knowing when the action would take place, could profit by making an accurate bet on the time of the subject's death. Because the payoff is for accurately picking the date rather than performing the action of the assassin, it is substantially more difficult to assign criminal liability for the assassination. There are reports of crowd funded assassinations and hitmen for hire, however, these are believed to be exclusively scams. The creator of Silk Road, Ross Ulbricht, was arrested by Homeland Security investigations (HSI) for his site and allegedly hiring a hitman to kill six people, although the charges were later dropped.

There is an urban legend that one can find live murder on the dark web. The term “*Red Room*” (Drazen, 2014) has been coined based on the Japanese animation and urban legend of the same name. However, the evidence points toward all reported instances being hoaxes. On June 25, 2015, the indie game *Sad Satan* was reviewed by Youtubers *Obscure Horror Corner* which they claimed to have found via the dark web. Various inconsistencies in the channel's reporting cast doubt on the reported version of events. There are several websites which analyze and monitor the deep web and dark web for threat intelligence, for example Sixgill.

Phishing and Scams

A phishing website (sometimes called a “spoofed” site Zarras et al, 2014) tries to steal your account password or other confidential information by tricking you into believing you're on a legitimate website. You could even land on a phishing site by mistyping a URL (web address). Phishing via cloned websites (Elangovan et al, 2019) and other scam sites are numerous, with darknet markets often advertised with fraudulent URLs.

Puzzles

1

Puzzles such as Cicada 3301 and successors will sometimes use hidden services in order to more anonymously provide clues, often increasing speculation as to the identity of their creators.

Illegal and Ethically Disputed Pornography

There is regular law enforcement action against sites distributing child pornography – often via compromising the site by distributing malware to the users (Mark, 2014). Sites use complex systems of guides, forums and community regulation. Other content includes sexualized torture and killing of animals and revenge porn.

Terrorism

There are at least some real and fraudulent websites claiming to be used by the Islamic State of Iraq and the Levant (ISIL) previously ISIS, including a fake one seized in Operation Onymous (Weimann, 2016). In the wake of the November 2015 Paris attacks, an actual such site was hacked by an Anonymous affiliated hacker group GhostSec and replaced with an advert for Prozac. The Rawti Shax Islamist group was found to be operating on the dark web at one time.

Social Media

Within the dark web, there exist emerging social media platforms similar to those on the World Wide Web. Facebook and other traditional social media platforms have begun to make dark-web versions of their websites to address problems associated with the traditional platforms and to continue their service in all areas of the World Wide Web.

CONCLUSION

The deep web will continue to perplex and fascinate everyone who uses the internet. It contains an enthralling amount of knowledge that could help us evolve technologically and as a species when connected to other bits of information. And of course, it's darker side will always be lurking too, just as it always does in human nature. The deep web speaks to the fathomless, scattered potential of not only the internet but the human race, too. Regardless of if the Dark Web exists or not, the aforementioned activities still occur. The Dark Web just provides an easy way to connect with people of similar interests and to facilitate further interaction.

REFERENCES

- Alrwais, S., Yuan, K., Alowaisheq, E., Li, Z., & Wang, X. (2014). Understanding the dark side of domain parking. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)* (pp. 207-222). Academic Press.
- Baravalle, A., Lopez, M. S., & Lee, S. W. (2016, December). Mining the dark web: drugs and fake IDs. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)* (pp. 350-356). IEEE. 10.1109/ICDMW.2016.0056
- Barford, P., & Yegneswaran, V. (2007). An inside look at botnets. In *Malware detection* (pp. 171-191). Boston, MA: Springer. doi:10.1007/978-0-387-44599-1_8
- Bergman, M. K. (2001). White paper: the deep web: surfacing hidden value. *The Journal of Electronic Publishing: JEP*, 7(1). doi:10.3998/3336451.0007.104
- Berners-Lee, T., Dimitroyannis, D., Mallinckrodt, A. J., & McKay, S. (1994). World Wide Web. *Computers in Physics*, 8(3), 298-299. doi:10.1063/1.4823300
- Biryukov, A., & Pustogarov, I. (2015, May). Bitcoin over Tor isn't a Good Idea. In *2015 IEEE Symposium on Security and Privacy* (pp. 122-134). IEEE. 10.1109/SP.2015.15
- Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Héту, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International*, 264, 7-14. doi:10.1016/j.forsciint.2016.02.045 PMID:26978791
- Brown, D. (2010). Resilient botnet command and control with tor. *DEF CON*, 18, 105.
- Chaum, D. (2003). Untraceable electronic mail, return addresses and digital pseudonyms. In *Secure electronic voting* (pp. 211-219). Boston, MA: Springer. doi:10.1007/978-1-4615-0239-5_14
- Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American Society for Information Science and Technology*, 59(8), 1347-1359. doi:10.1002/asi.20838
- Cubrilovic, N. (2014). *Large number of tor hidden sites seized by the fbi in operation anonymous were clone or scam sites*. Retrieved from <https://www.nikcub.com/posts/onymous-part1>
- Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Naval Research Lab. doi:10.21236/ADA465464
- Drazen, P. (2014). *Anime Explosion!: The What? Why? and Wow! of Japanese Animation*. Stone Bridge Press.
- Elangovan, R., & Prianga, M. (2019). Side Channel Attacks in Cloud Computing. In *Cognitive Social Mining Applications in Data Analytics and Forensics* (pp. 77-98). IGI Global. doi:10.4018/978-1-5225-7522-1.ch005
- Gibbs, S. (2018). Silk Road underground market closed – but others will replace it. *The Guardian*.
- Guarineri, C. S. (2012). *a Tor-powered botnet straight from Reddit*. Academic Press.
- Kiss, J. (2013). Tor 'deep web' servers go offline as Irish man held over child abuse images. *The Guardian*.

- Manikandakumar, M., & Ramanujam, E. (2018). Security and Privacy Challenges in Big Data Environment. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 315-325). IGI Global. doi:10.4018/978-1-5225-4100-4.ch017
- Marin, E., Diab, A., & Shakarian, P. (2016, September). Product offerings in malicious hacker markets. In *2016 IEEE conference on intelligence and security informatics (ISI)* (pp. 187-189). IEEE. doi:10.1109/ISI.2016.7745465
- Mark, W. (2014). *Tor's most visited hidden sites host child abuse images*. BBC News.
- Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer. doi:10.1057/9781137399052
- Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 58(1), 7–38. doi:10.1080/00396338.2016.1142085
- Munson, L. (2013). *Tor usage doubles in August. New privacy-seeking users or botnet*. Academic Press.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Academic Press.
- Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *The International Journal on Drug Policy*, 24(5), 385–391. doi:10.1016/j.drugpo.2013.01.005 PMID:23465646
- Weimann, G. (2016). Terrorist migration to the dark web. *Perspectives on Terrorism*, 10(3).
- Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C., & Vigna, G. (2014, November). The dark alleys of madison avenue: Understanding malicious advertisements. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (pp. 373-380). ACM. 10.1145/2663716.2663719

Privacy, Ethics, and the Dark Web

Richard T. Herschel

Saint Joseph's University, USA

INTRODUCTION

Online activities that have compromised people's privacy has led to the creation of legislation that is intended to protect privacy rights. These decrees represent an attempt by law enforcement and government officials to more forcefully address immoral patterns of online behavior that are effectively compromising the safety of society. Two primary examples of this new legislation are the European Union's General Data Protection Regulation [GDPR] and the California Consumer Privacy Act. Both detail rules and procedures that organizations must follow when handling the personal information that they collect online as well as the rights afforded to the individual in the management of their digital identity.

The GDPR states that EU citizens have the right to information about them that is being collected by organizations as well as how it is being processed. They can ask that incorrect, inaccurate, or incomplete personal data be corrected or that their personal data be erased. Individuals can restrict the processing of their personal data for marketing purposes or for any other given situation they deem necessary. People can even request that decisions based on automated processing concerning them be made by people, not only by computers (EU Commission (1), 2018). The GDPR defines personal data to include any information generated by organizations that monitors citizen behavior and generates personal information. This includes all forms of tracking and profiling on the internet, including for the purposes of behavioral advertising.

California has passed new consumer-privacy legislation that is somewhat similar to the GDPR - California Consumer Privacy Act, A.B. 375. This law is the first of its kind in the United States. The California regulation requires businesses to offer consumers options to opt out of the sharing of their personal information, and it gives Californians the right to prohibit the sale of their personal data. The law also forbids retailers from treating customers who opt out of data sharing any differently from those who don't, suggesting the possibility that this provision could end loyalty programs that offer discounts to members. The regulation broadens the definition of what constitutes personal information and it gives enforcement power to the California attorney general (Vartabedian, Wells, and O'Reilly (2018).

While these legislative actions are intended to constrain organizations in their use of personal information collected online, there remains a high probability that continuing attempts will be made to compromise data privacy. Specifically, the illicit activities of entities employing the Dark Web present an ongoing and much more serious challenge to the protection of privacy rights than do the activities of legitimate organizations engaged in online business transactions.

Primarily off the mainstream radar until recently, the Dark Web is viewed by many as a haven for those who engage in unscrupulous behavior. Yet, at the same time it can also provide an important safe harbor for those engaging in whistleblowing activity. This paper examines the challenges that the Dark Web presents for society, its impact on privacy rights, and the ethical challenges that require organizations to be vigilant in order to minimize threats to both their clientele and to their operations. The paper also examines the important role that ethical theories play in shaping our views about Dark Web activities.

DOI: 10.4018/978-1-5225-9715-5.ch009

BACKGROUND

1

Hartnett (2017) states that when someone refers to doing online research on a topic or they are looking for other online information, they typically use search engines such as Google, Yahoo, Safari, and Bing. These applications employ information on the public [or surface] web, which represents only 4% of web content (~8 billion pages). The Deep Web refers to the other 96% of the digital universe that is basically hidden. Wolford (2018) notes that this is the bulk of the Internet and it differs from the surface internet that most people know and use, because it is not indexed by search engines. He reports that the Deep Web includes content such as financial databases, web archives, and secured documents.

Hewilson (2018) provides some interesting statistics about the Deep Web. The author reports that:

- the Deep Web contains 7500 terabytes of information where the surface web, in comparison, contains 19 terabytes of content,
- the Deep Web has between 400 and 550 times more public information than the surface web,
- more than 200,000 Deep Web sites currently exist,
- together, the 60 largest Deep Web sites contain around 750 terabytes of data, surpassing the size of the entire surface web 40 times,
- 550 billion individual documents can be found on the Deep Web compared to the Surface Web's 1 billion individual documents, and
- 95% of the Deep Web is publicly accessible, meaning no fees or subscriptions.

Pagliery (2014) contends that the vast majority of the Deep Web holds pages with valuable information. He states that 54% of Deep Web websites are databases. These include, he states, those of the U.S. National Oceanic and Atmospheric Administration, NASA, the Patent and Trademark, and the Securities and Exchange Commission's EDGAR search system -- all of which are public. However, it also includes, he notes, pages kept private by companies that charge a fee to see them, like the government documents on LexusNexus and Westlaw or the academic journals on Elsevier.

The Dark Web of the Deep Web

Embedded in the Deep Web is the Dark Web. Chertoff (2017) states that The Dark Web is a very small, hard-to-access portion of the Deep Web. He says that it accounts for less than 0.01% of the sites on the Internet. Bischoff (2018) agrees that the Dark Net is a small part of the Deep Web. In the Dark Web, he asserts, are users who are deliberate in their desire to be free from the prying eyes of governments and corporations because they deliberately need to mask their identities and as well as their illicit activities.

The British Computing Society (2017) describes what some of these unscrupulous activities include:

- **Forums:** They state that discussion forums here provide a way for criminals and other people to communicate and share information with each other. They assert that many criminal conspiracies are in all likelihood planned and carried out because of conversations which take place on the Dark Web forums.
- Software downloads and serial key sharing. Downloading illegal software, and sharing serial keys is commonplace throughout the Dark Web, allowing some people to gain access to software for nothing.

- **Hackers:** The Dark Web is a marketplace for hackers to buy and sell their services, as well as to talk. Here hackers communicate with people who want to buy their services, commonly via forums.
- **Illegal Items of all Types:** The Dark Web marketplace offers everything from hitmen to drugs to counterfeit currency.

HuntSource (2018) notes that contrary to popular belief, browsing the Dark Web is not illegal in and of itself, unless you access sites with forbidden content or purchase contraband, stolen or forbidden products in the plethora of digital marketplaces that are found there. Glance (2018) reports that “darknet markets” sell illegal products like drugs and firearms, paid for in the cryptocurrency Bitcoin. In addition, he says it is a place used by pedophile groups, terrorists, and criminals to keep their dealings secret and it is the place of choice for groups wanting to stay hidden online from governments and law enforcement agencies and where whistleblowers communicate with journalists.

Stack’s (2018) data provides an interesting list of the most common pieces of information sold on the Dark Web and their prices:

- Social security number \$1
- Online payment services login info \$20-\$200
- Driver’s License \$20
- Loyalty Accounts \$20
- Diplomas \$100-400
- Passports (U.S.) 1000-2000
- Credit or debit cards: \$5 with CVV number, \$15 with Bank info, \$30 with complete detailed information
- General non-financial institution logins \$1
- Subscription services \$1-\$10

Medical records \$1-\$1000

Osborne (2018) says that stolen airline mileage is also offered for sale on the Dark Web at a fraction of its true cost -to the detriment of their true owners. Osborne reports that 100,000 BA air miles were found for sale at the price of €124 (\$144); 45,000 Delta SkyMiles could be bought for \$101; 100,000 Emirates Skywards points could be purchased for \$520, and \$884 would buy you 100,000 Virgin Atlantic Flying Club points. These air miles are offered for purchase using cryptocurrency (e.g., Bitcoin).

Brewster (2018) reports that a recently developed map of the Dark Web shows 6,608 dark web sites crawled during January of 2018. He states that this includes all manner of webpages, from the amusing to the horrific. Amongst the myriad pages on the map, he says there is clear evidence of extreme sexual content, credit card cloning products, a large number of Bitcoin scams, and an assortment of whistleblower pages.

C.M. (2018) concurs that the emergence of the Dark Web has led to increasingly malicious activities on the Internet that has impacted the effectiveness of cybersecurity and Internet governance. He argues that cybersecurity aims to protect information systems and data for any organization, while Internet governance is comprised of the evolving policies and rules under which online users make decisions on Internet use and development. These two bodies have been put in place to ensure that the integrity of the use of the Internet is considered by any user and to ensure that no illegal operations take place.

However, on the Dark Web, he states, ill-intentioned entities can transmit false information and even plan unlawful attacks against a government, and this creates challenges to their Internet governance and cybersecurity control centers. And, C.M. reports that further compounding the problem is the fact that the number of hackers carrying out their activities on the Dark Web is rapidly rising and more people are employing the use of cyberattack services or even learning how to manage it for themselves without being tracked. The bottom line is that the Dark Web provides a favorable environment for conducting illegal businesses and this reduces trust in all forms of business conducted on the Internet.

PRIVACY PROTECTION AND THE DARK WEB

Because of the vulnerability that the Deep Web presents for organizations, it can become a complicating factor in establishing GDPR compliance. If, for example, personal data held by a firm is hacked and then the data leaked, organizations must make every effort to inform the EU of the suspected breach, assuming that they themselves are aware that it has occurred. Once data appears on the Dark Web, it may be ruled as visible under the GDPR and be grounds for penalization.

Bonilla (2018) notes that as data grows in value, attempted cybersecurity breaches for the sake of mining sensitive information will only increase. With many networks having loopholes that can be exploited quietly by hackers using techniques such as phishing, data can be stolen without any major signs that a breach occurred. This means that to maintain compliance with the GDPR, firms will have to proactively determine if those whose data they collect have ever been the victim of a data breach. And, he notes, that is easier said than done.

PAConsulting (2018) states that the National Security Agency (NSA) and UK Government Communications Headquarters (GCHQ) have devoted considerable effort and resources to infiltrating what occurs on the Dark Web. But in response to this, PAConsulting reports that Dark Web activists who want to stop government ‘spying’ on people are developing a wide range of tools to thwart this infiltration. These protesters are advocating the use of strong cryptography and privacy-enhancing technologies – software that ensures complete anonymity in activities that activists employ to foster social and political change. However, PAConsulting notes that criminal groups and terrorists will also use these tools to commit illegal acts undetected.

The widespread availability of Dark Web forums dedicated to freely sharing privacy-enabling technologies, intrusion software, and exploitable code means that global law enforcement agencies face an uphill struggle. PAConsulting reports that the sheer complexity of the Dark Web means it is unlikely that hacktivist groups will be regulated any time soon. In the meantime, criminal groups can arm themselves with freely-available technologies that are making their job even easier, and their victims’ job all that more difficult. PAConsulting concludes there is a growing number of technically-savvy ‘amateur hackers’ carrying out cyber-attacks, though with relatively little impact. But they caution businesses to be wary that even the average customer could buy a cyber-attack service anonymously – or possibly learn to conduct their own cyber-attack – without being caught.

Kang (2018) states that companies and individuals that don’t have the ability to monitor the Dark Web for stolen information can turn to specialized entities and agencies that do. He notes that the credit monitoring company Experian recently launched a Dark Web monitoring service for individuals and he indicates that other companies may soon follow suit. He reports that businesses have more options. He notes, for example, that the National Cyber & Forensics Training Alliance, a nonprofit information sharing organization affiliated with the FBI offers a free Internet Fraud Alert program that provides busi-

nesses with a degree of Dark Web monitoring. Companies requiring personalized levels of monitoring can pay for services from a number of forensic firms.

Kang offers that if individuals and companies learn that their personal or business information has been spotted on the Dark Web, their next step is to minimize damage. He says that individuals can change login passwords or cancel compromised financial accounts and businesses can similarly instruct employees to change compromised credentials, and they can begin investigating their company's systems for infiltration in order to plug holes. Finally, Kang says, that knowing you're your company's (or personal) information was stolen gives a reason to contact law enforcement. He encourages victims to report theft of online information to organizations like the FBI. He says that they can do this at either an FBI Office or online via the Internet Crime Complaint Center. He urges both individuals and businesses to do so, because providing this information may help law enforcement to develop trends and patterns to find criminal actors.

Kang (2018) does acknowledge that in the right hands, the Dark Web can be used to foster positive social change. For example, he notes that democracy activists in foreign countries have used the anonymity of the Dark Web to organize their activities and, he says, the United States State Department has invested time and resources to encourage this use of the Dark Web.

Corse (2018) reports that with elections, one issue looms large for voters and election officials alike: cybersecurity. Hoping to quell fears about foreign hackers and repel potential threats, he reports that many states and counties are beefing up their plans to deal with cyberattacks. Corse says that they work to shore up systems to protect voter databases, hiring security experts to assess the strength of their defenses. He reports that officials coordinate with social-media organizations to stamp out deliberately fraudulent messages that could mislead voters about how to cast a ballot. And, he says, they band together to share information and simulate how they would respond to potential emergencies. Course reports that one simulation-based exercise, held by the Department of Homeland Security in mid-August of 2018, gathered officials from 44 states, the District of Columbia and multiple federal agencies.

The cost of protecting privacy is significant. Steve (2018) reports that the government of Canada is allocating one billion dollars to their federal budget to be spent on the fight against cybercrime. The Republic of Canada in the recent past has experienced an increased number of cyberattacks directed at its vital institutions, including hospital networks and government agencies. Officials fully expect that hackers will continue to engage in cybercrime activities via the Dark Web.

Pepper (2018) reports that Australia has introduced an Assistance and Access Bill to secure critical support from the communications industry that will enable law enforcement to effectively investigate serious online criminal activity. The legislation notes that encryption conceals the content of communications and data held on devices, as well as the identity of users and that secure encrypted communications are increasingly being used by terrorist groups and organized criminals to avoid detection and disruption. Pepper states that the bill seeks to grant the Australian authorities' clear powers to carry out stealthy surveillance activities on electronic devices and it prompts tech organizations to cooperate in decrypting private communications.

Thales (2018) provides data that reveals how challenged organizations are in dealing with threats to the privacy of their information. They conducted a poll of 1,200 organizations that revealed the following descriptive statistics concerning privacy protection issues:

- 42% of enterprises breached this year had been breached in the past.
- 79% increased IT security spending – and the data breaches didn't even slow down.

- 78% of the organizations plan increasing security spending in 2018, including 86% of U.S. organizations, up from 73% globally in 2017.
- Percentage of global organizations who state that they will not be impacted by data privacy/sovereignty regulations (e.g., GDPR) was 28% 2017, 13% in 2018

OWL Cybersecurity (2018) employed data and analytics to generate a darknet footprint of Fortune 500 companies that provides a snapshot view of each company's exposure on the darknet relative to its peers. Their analyses revealed that the highest scoring companies all had credentials and/or intellectual property exposed on the darknet that could be monetized by others. They also discovered that every Fortune 500 company had a positive darknet Index score, meaning they have a presence on the darknet. The company with the largest darknet footprint was found to be Amazon. However overall, technology and telecommunications companies were seen as the largest target as they were had the highest Darknet Index scores, indicating that they are the most attractive firms targeted by threat actors.

PRIVACY, ETHICS, AND THE DARK WEB

Richard (2018) defines privacy as a state in which an individual is able to hide information about themselves for no reason other than to keep it from others. When you lack online privacy, he says, it means that all your information can be accessed, either willingly or forcibly. Anonymity, on the other hand, is the ability to hide one's true identity from others, chiefly to remain unknown without hiding or censoring their activities. Richard asserts that while anonymity might not be as inherent as privacy, it is just as important in any society, because it enables activists and whistleblowers to say what many would otherwise not say for fear of retribution. Hence, he believes that the anonymity provided by the Dark Web provides activists with a measure of protection from powerful corporate and political enemies. Without it, he says, few would be willing to come forward.

The University of Warwick and TNO (2017) provide arguments that are sympathetic with those presented by Richard. They note that technology commentators and researchers routinely predict that web activity will increasingly migrate to the Dark Web as people become more concerned about their privacy and less tolerant of corporate monitoring of their behavior for marketing purposes. Privacy and censorship concerns, they say, are emerging as significant predictors of reduced opposition to the Dark Web where anonymity helps to protect one's privacy.

The University of Warwick and TNO believe that people's Dark Web activities are not only innocuous, but they also constitute the exercise of their valuable freedoms. Chief amongst these, they say, are the freedom to express political views or sexual preferences without fear of persecution by authoritarian regimes and the freedom to exchange information without manipulation or monitoring by profit-seeking companies. The authors contend that some Dark Web users consider the term 'dark net' or 'Dark Web' itself a media fabrication to draw attention away from the legitimate, innocuous, and even life-saving use of the Dark Web and towards those that are criminal. Some, they say, like Edward Snowden and Julian Assange, see government-sponsored attempts to crack anonymity on the Dark Web as an attack on freedoms, especially privacy.

The University of Warwick and TNO suggest that a law enforcement approach to the Dark Web that treats all activity there as suspect in an undifferentiated, blanket manner risks undermining the exercise of these freedoms. They contend, for example, that attempting to crack encryption and expose the iden-

tities of individuals interacting anonymously on the Dark Web might not only expose those particular individuals to harm from authoritarian governments, but also undermine the trust that is vital to the effective function of the Dark Web as a space safe from political persecution. For this reason, they suggest that law enforcement organizations in liberal democratic jurisdictions adopt a targeted approach to policing the Dark Web, focusing on exposing, disrupting and prosecuting criminals while refraining from interfering with innocuous activities and the exercise of political freedoms.

ETHICAL THEORIES

Ethical theories can be useful in helping to articulate people's judgments when they examine the morality of the activities of the Dark Web and means for intervening to constrain controversial behavior. Ethical theories provide a foundation for a reasoned moral argument and they provide a basis for legitimacy since they are rooted in ethical philosophy.

Sound ethical theories share a common property. They enable an individual to make persuasive, logical, and reasoned arguments based on the principles stated by the ethical theory. To illustrate this, two ethical theories, Kantianism and Utilitarianism, will be briefly described and then used to see how an ethical argument about the Dark Web might be framed.

Kantianism

Kantian ethics, originating with the German philosopher Immanuel Kant (1724-1804), is an ethical theory concerned about not what we do, but what we ought to do -- our dutifulness. Dutifulness reflects good will, which is the desire to do things right based upon rules that everyone ought to follow. That is, a dutiful person acts the way they do because of a moral rule. Moral rules are imperatives that are either hypothetical or categorical and they are the means by which reason commands our will and our actions. Hypothetical imperatives equate to conditional if, then statements relative to what you are trying to accomplish. Categorical imperatives command unconditionally as they are unequivocal. For Kant, rules are paramount. Everyone is held to the same standard and there are clear guidelines for appropriate behavior. Hence, in Kantianism it is not the outcome of a behavior that matters. It is the intent, the rule behind the action, that is most critical (California State University Sacramento, 2016).

One Kantian categorical imperative states that one should always respect the autonomy of other people, treating them as ends in themselves and never only as means to an end. With the Dark Web, this would be a difficult case to make. Since some activity on the Dark Web routinely involves compromising a target's privacy without their consent, these Dark Web participants are not respecting the autonomy of people and they are in fact using others personal data as a means to an end to further their own self-interest. Moreover, because they engage in their Dark Web activity anonymously, one could also judge this to be problematic. With Kantianism, you want everyone to act as you want all people to act towards all other people. In the Dark Web instance, where everyone is anonymous and thereby compromising the transparency of sources, there is no opportunity for anyone to value a source and hence to trust their intentions. Overall then, the intent to hide one's identity from others is not something which one would want to apply universally to every situation. However, there are exceptions such as the instances where whistleblowers require concealment with their intent to act in the common good. Here the morality of

these Dark Web activities might be justified through the use of a Kantian hypothetical imperative. That is, if the intent of the use of anonymity by a whistleblower is to afford the expression of information that promotes the common good, while also protecting them from oppression and harm, one could state this is morally justified.

Utilitarianism

Unlike Kantianism, Utilitarianism [originating from Jeremy Bentham (1748-1832) and John Stuart Mill (1806-1873)] examines right or wrong based on the consequences of an act or a rule. The act utilitarian perspective applies the principle of utility to individual moral actions and the rule utilitarian applies the principle of utility to moral rules. The right act is one that produces the greatest happiness for a community or society. A wrong act decreases the total happiness of the affected parties. The right moral rule of conduct is one where if it is adopted by everyone, will lead to the greatest net increase in happiness for all involved. Hence, in the utilitarianism ethical perspective, one must calculate what action or rule achieves the best results. That is, one must account for and weigh the good and the bad elements affecting a situation to determine the net consequences of the action or rule. Unlike the Kantian perspective where the focus is upon examining the will that motivates action, it is the “happiness” or the maximum well-being outcome that is most critical in Utilitarianism (Cavalier, 2002).

Applying the Utilitarian perspective can be fraught with complications. It requires that acts and rules be assessed using a utilitarian calculus where the good and bad of the Dark Web would be weighed on a scale. From an Act Utilitarian perspective, for example, one would have to quantify the plusses and minuses of Dark Web consequences relative to such factors as the intensity of the experience, its duration, the financial consequences of the action(s), the number of people positively and negatively impacted, and the potential of this activity and/or entity to produce more experiences of the same kind. To decide whether the action of Dark Web actors is right or wrong, one must total the positive and negative consequences to all of those being affected and choose the alternative with the highest total score.

The major potential drawback of this approach may be the potential ambiguity and biases inherent in trying to identify and quantify both the pros and cons of Dark Web activity and behavior. Trying to reach consensus as to the intent and impact of the Dark Web can be problematic since the costs and benefits in the analysis would have to be quantified to a common economic unit of analysis. And in doing the assessment, bias may be made manifest via selectivity in what data is selected and how it is weighted.

That said, the principles of Utilitarianism are typically applied in assessing the impact of the Dark Web. Where Kantianism might confine us to assessing the intent of a Dark Web actor on a case by case basis, Utilitarianism provides a basis for enabling a calculation that expresses a judgement of the overall consequences of Dark Web activity on the public, which then can be used to justify the value (and the expense) of the government legislation and the cybersecurity measures that are implemented to protect citizenry and their privacy from Dark Web activity.

SOLUTIONS AND RECOMMENDATIONS

Privacy is a something that people intrinsically want to protect. Ethics provides moral justification for explaining why. The Dark Web challenges both. It is a frontier not unlike the Wild West.

Ethical theories such as Kantianism and Utilitarianism, help us to understand and articulate the moral issues inherent in both the intent and the consequences of the illicit behavior being manifested on the Dark Web. And clearly, there real data privacy issues that have had moral, legal, and economic consequences. At the same time however, there are also innocuous and even positive behaviors that occur in the Deep Web space.

Hence it is important going forward to monitor the ethical and social consequences that the distribution of anonymous browsers and the widespread availability of open networks create. While there is extensive interest now in our cybersecurity, we should also stay cognizant of the fact that some of the activities of the Dark Web may have a positive effect on societal behavior. Clearly hacking is an activity with no moral justification. The goodness of whistleblowing, however, is not so easy to assess. From the perspective of Kantianism, one must assess the goodness of the whistleblower's intentions. And Utilitarianism demands that we systematically evaluate whether the impact of the whistleblowing was positive or negative for the majority of the citizens who were targeted by its action.

Unfortunately, most of us only consider the ethics of a situation when we have been made aware that there is a problem. Typically, we are too trusting that somehow online entities will respect our data privacy. Sometimes we are simply too ignorant of potential threats or too busy to manage our online activities with due diligence.

Government rules mandating strict data management policies were therefore probably inevitable. The idea that firms will self-regulate has been shown not to work well. There was and is a gold mine of online data for firms to harvest and analytics can tell them more about people's behavior than they ever knew to ask. In the process of doing this, the deliberate or unintentional misuse of personal data became inescapable. New privacy laws are a clear admission that something has been wrong and that individuals are basically powerless to control how their private information is shared.

To expect consistent ethical behavior online has been shown to be wishful thinking. In fact, with the Dark Web, ethical behavior is seen by many to be an oxymoron. Eventually, the future of the Dark Web may depend how much society will tolerate anonymous, unregulated free speech. Hence, it is probably prudent that we should monitor current and future Internet regulations. I think it is important to recognize when legislation may be compromising the actions of those with good intentions when its actions are trying to fix behaviors that it judges to be morally wrong.

FUTURE RESEARCH DIRECTIONS

As we move forward, we must be highly attentive to how we deal with the Dark Web. What we do to it and how we do it will tell us as much about ourselves as about it. If we work to aggressively stamp out all criminal behavior, we might inadvertently silence important voices that needed this platform's anonymity for safety from oppressors. It is a balancing act that will require careful thought and reflection as we are actively trying to attend to our cybersecurity. What ethics tells us is that we should stop to consider whether using a scalpel would be better than using a hatchet when dealing with Dark Web issues and it will help us to understand why. Ongoing research will be needed to document and explore the arguments that will be voiced. In doing so, we can examine whether these judgements are grounded in the reasoned moral arguments of ethical theory.

REFERENCES

- Bischoff, P. (2018, September 12). Step by step guise to safely accessing the dark net and deep web. *VPN & Privacy*. Retrieved from <https://www.comparitech.com/blog/vpn-privacy/how-to-access-the-deep-web-and-darknet/#gref>
- Bonilla, H. (2018, April 20). Dark Web breaches can affect your compliance with GDPR. *SWK Network Services*. Retrieved from <https://www.swknetworkservices.com/dark-web-breaches-compliance-gdpr/>
- Brewster, T. (2018, March 13). This insane map shows all of the beauty and horror of the Dark Web. *Forbes*. Retrieved from <https://www.forbes.com/sites/thomasbrewster/2018/03/13/dark-web-map-6000-webpages/#2f26b53018e7>
- British Computing Society. (2017, May). Demystifying the Dark Web. *British Computing Society*. Retrieved from <https://www.bcs.org/content/conWebDoc/57766>
- California State University Sacramento. (2016). *Kantian ethics*. Retrieved from <http://www.csus.edu/indiv/g/gaskilld/ethics/kantian%20ethics.htm>
- Cavalier, R. (2002). *Online guide to ethics and moral philosophy: Utilitarian theories*. Retrieved from <http://caae.phil.cmu.edu/Cavalier/80130/part2/sect9.html>
- C.M. (2018, May16). Impact of the Dark Web on cybersecurity and Internet governance. *DarkWebNews*. Retrieved from <https://darkwebnews.com/dark-web/impact-of-darkweb-in-cybersecurity-and-internet/>
- Commission, E. U. (2018). What are my rights? *European Commission Policies, information and services*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en
- Corse, A. (2018, September 18). The Cyberthreat's that most worry election officials. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/the-cyberthreats-that-most-worry-election-officials-1537322820>
- Cybersecurity, O. W. L. (2018). The OWL Cybersecurity Darknet Index. *Owlcyber.com*. Retrieved from https://static1.squarespace.com/static/5724ee301bbee056721dd394/t/591b834c893fc044ddce42e9/1494975310906/OWL_Cybersecurity_Darknet_Index.pdf
- Glance, D. (2018). What is the Dark Web? *IFLScience*. Retrieved from <https://www.iflscience.com/technology/what-dark-web/all>
- Hartnett, T. (2017, March 1). Meet the newest ethical and legal challenge of obtaining and using data via the internet: The dark web. *CenterWatch*. Retrieved from <https://www.centerwatch.com/news-online/2017/03/01/meet-the-newest-ethical-and-legal-challenge-of-obtaining-and-using-data-via-the-internet-the-dark-web/>
- Hewilson. (2018). *The Deep Web: Statistics*. Retrieved from <https://hewilson.wordpress.com/what-is-the-deep-web/statistics/>
- HuntSource. (2018, January 15). Cyber security and the Dark Web. *HuntSource*. Retrieved from <https://huntsource.io/cyber-security-dark-web/>

Kang, R. (2018, January 23). Welcome to the dark Web: A plain English introduction. *IAPP*. Retrieved from <https://iapp.org/news/a/welcome-to-the-dark-web-a-plain-english-introduction/>

Osborne, C. (2018, September 19). Hackers peddle thousands of air miles on the Dark Web for pocket money. *ZDNet*. Retrieved from <https://www.zdnet.com/article/hackers-peddle-thousands-of-air-miles-on-the-dark-web-for-pocket-money/>

PAConsulting. (2018, September 20). Why the ‘dark web’ is becoming a cyber security nightmare for businesses. *PA Opinion*. Retrieved from <https://www.paconsulting.com/insights/why-the-dark-web-is-becoming-a-cyber-security-nightmare-for-businesses/>

Pagliery, J. (2014, March 10). The Deep Web you don’t know about. *CNNtech*. Retrieved from <https://money.cnn.com/2014/03/10/technology/deep-web/index.html>

Pepper, C. (2018, September 3). Analysis: Australia’s Proposed Cybersecurity Bill & its implications for Privacy. *DarkWebNews*. Retrieved from <https://darkwebnews.com/cyber-security/au-cybersecurity-bill>

Richard. (2018, February 9). Privacy vs. Anonymity. *DarkWebNews*. Retrieved from <https://darkwebnews.com/anonymity/privacy-vs-anonymity/>

Stack, B. (2018, April 9). Here’s how much your personal information is selling for on the Dark Web. *Experian*. Retrieved from <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

Steve. (2018, March 21). Canada allocates \$1 Billion to Safeguard against cybercrime. *DarkWebNews*. Retrieved from <https://darkwebnews.com/cyber-security/1-billion-against-cybercrime-canada/>

Thales. (2018). 2018 Thales data threat report global edition. *Thales*. Retrieved from https://dtr.thalesecurity.com/?utm_source=google&utm_medium=cpc&utm_campaign=DTR&utm_term=%7BKeyword%7D&gclid=EAIaIQobChMIImZPBncjH3QIVEInCh1hCAMEEAMYASAAEgKN8_D_BwE

University of Warwick & TNO. (2017). Policing the Dark Web: Ethical and legal issues. *Medi@4SEC*. Retrieved from <http://media4sec.eu/downloads/d4-3.pdf>

Vartabedian, M., Wells, G., & O’Reilly, L. (2018, July 1). Businesses Blast California’s New Data-Privacy Law. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/businesses-blast-californias-new-data-privacy-law-1530442800>

Wolford, B. (2018, August 27). What is the dark web? The good and bad of the Internet’s most private corner. *ProtonMail*. Retrieved from <https://protonmail.com/blog/what-is-dark-web/>

ADDITIONAL READING

Bruno. (2018, January 23). How to monitor the Dark Net for business threat intelligence. *DarkWebNews*. Retrieved from <https://darkwebnews.com/cyber-security/how-to-monitor-darknet-for-business-threat-intelligence/>

Cipher. (2014, December 22). The ethics of the Deep Web. *Deep.Dot.Web*. Retrieved from <https://www.deepdotweb.com/2014/12/22/ethics-deep-web/>

Curran, D. (2018, July 24). My terrifying deep dive into one of Russia's largest hacking forums. *The Guardian*. Retrieved from <https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety>

Quinn, M. J. (2017). *Ethics for the Information Age*. Hoboken, NJ: Pearson.

Dark Web: A Boon or a Bane

Punam Bedi

 <https://orcid.org/0000-0002-6007-7961>

University of Delhi, India

Neha Gupta

University of Delhi, India

Vinita Jindal

 <https://orcid.org/0000-0002-0481-4840>

Keshav Mahavidyalaya, University of Delhi, India

INTRODUCTION

Ever since its conceptualisation, the Internet has revolutionised the way people live. From faster communication to convenient information sharing, the human race has been abundantly blessed by the applications of the Internet. Most people today, mainly use the Internet for accessing various websites or web pages containing different forms of information – like text, image, audio, video etc. Such widespread use of the Internet for data retrieval purpose, has got people thinking about the difference between the Internet and the World Wide Web (or simply the Web). In essence, the Internet comprises of networks across the world, interconnected together to form one massive global network. These networks are connected via cables or satellite links and follow a predefined set of rules for communication, called protocols. The Internet uses different protocols to deliver a variety of services to its users – like data dissemination, email, file sharing, online messaging etc. Out of all such services the World Wide Web only provides data dissemination or information sharing capability to the Internet. It allows web pages to display content present on world's different networks by using Hyper Text Transfer Protocol (HTTP). Services like email and file sharing, which are not a part of the World Wide Web, are governed by Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and File Transfer Protocol (FTP) respectively. Since users mostly access the Web portion of the Internet to share and/or retrieve information, the two terms – the Web and the Internet - are used interchangeably by common people. But these two terms are not synonymous. The Internet is the underlying (hardware) infrastructure over which the World Wide Web (software) hosts digital content in the form of websites or simply web pages.

SURFACE WEB

The Web provides its users with billions of web pages that can be easily accessed via standard web browsers and search engines. This part of the Web which is openly available to everyone is known as the Surface Web (Santos, 2015). Users access online resources present on Surface Web by either typing

DOI: 10.4018/978-1-5225-9715-5.ch010

a Uniform Resource Locator (URL) in the web browser or submitting a string of keyword(s) to query the search engine. The latter option provides them with an ordered list of search results that are most relevant to their search query. Both these methods allow quick and easy access to information on the Surface Web - also known as Visible Web or Clearnet. With huge amounts of information lying just a few clicks away, the general audience tends to think that all online content hosted on the World Wide Web is part of the Surface Web and can be accessed by them through conventional search engines (like Google and Bing) and web browsers. But this is far from the truth. The Surface Web contains less than 20 percent of the total information present on the Web (Santos, 2015) (Sui, Caverlee, and Rudesill, 2015). This is because the Visible Web is solely formed by the contents that search engines are able to reach on the Web. Any web resource that is beyond the reach of search engines, is not a part of the Visible Web. Thus the volume of content present on the Surface Web is limited by the techniques that search engines follow to extract information from the World Wide Web.

Search engines make use of application programs that scan the World Wide Web to create an index of all “reachable” web resources. These programs are known as crawlers/spiders/harvesters. Crawlers navigate the Web to gather documents and files present online in the form of web pages. Usually, web pages are linked to each other via incoming and outgoing hyperlinks. These hyperlinks enable search engines’ spiders to reach different web pages and extract information from them. This process of gathering information while moving from one web page to another through hyperlinks, is known as crawling. Beginning with an initial set of seed URLs, a crawler scans every web page linked to these URLs via outgoing hyperlinks (Santos, 2015). All online content that is reachable via incoming and/or outgoing hyperlinks gets crawled. The crawled pages are then indexed to allow easy retrieval for later purposes. Finally, when the user submits a search query, the search engines display these indexed web pages in an ordered manner.

Though search engines have made a lot of information available, but a very large portion of the Web still remains inaccessible to users. This is because web spiders can only enter and leave web pages via hyperlinks. Web pages which do not have incoming hyperlinks cannot be reached by crawlers. Such pages remain un-crawled and their content remains hidden from the eyes of search engines’ spiders. This is why the number of web pages on the Surface Web is a subset of web pages available on the World Wide Web. The Web is an ocean of knowledge and crawlers dive into it to gather as much content as possible. Contents gathered by crawlers form the Surface Web while the remaining contents form a separate layer of the Web, called the Deep Web.

DEEP WEB

The World Wide Web is a collection of enormous data both accessible directly and not accessible directly through crawlers. The accessible data, which is indexed by standard search engines, forms the visible tip of the iceberg whose major portion lies unseen in the deeper layers of the Web. This “unseen” portion of the Web which cannot be indexed by traditional search engines is referred to as the Deep Web. It consists of all those contents that cannot be crawled by search engines’ spiders and hence does not appear in search results. Though Deep Web content remains hidden from regular searches, it is not usually illegal or dangerous, it is just made to be unsearchable. Most of this information can be displayed as a result of a targeted search over the Web. Deep Web, popularly known as the Hidden Web or Invisible Web,

contains a variety of information including academic records, conference proceedings, legal documents, medical data, corporate data, scientific findings, database contents, confidential citizen data protected by governments, information present in universities' library websites and any online information that is accessible only by registered individuals. This type of Deep Web data is generally found in:

- **Unlinked Web Content:** Any web page that is not linked with other web pages through backlinks (incoming and/or outgoing hyperlinks) remains veiled and it only becomes visible if the exact URL is known.
- **Dynamic content:** Websites that provide users with search boxes (instead of hyperlinks) to navigate among pages of a website, become a part of Deep Web. This category also includes information that is made accessible only after user fills an online form.
- **Private Content:** Deep Web also includes contents present on websites and networks, owned by governments, educational institutions and private organisations, that require registration and login to be accessed (Norton, 2016). For example, accounts created by users on online social networking websites, bank websites and even e-commerce sites are not returned in results of search engines.
- **Paid Services:** Another kind of un-crawled content includes paid services that are made available to authorised individuals only (Cooper and Chikada, 2015). For example: Paid video-streaming platforms.
- **Limited Access Websites/Web Pages:** All online material that requires human verification (like CAPTCHAs) before being displayed, remains unindexed and hidden from Surface Web (Santos, 2015).
- **Restrictions by Website Developers:** Web spiders (crawlers) can be prohibited from crawling a website if appropriate settings are made in the associated robots.txt file (Santos, 2015).
- **Limited-Access Networks:** This covers all those resources and services that are not reachable with standard network configurations. For example: sites with domain names that have been registered on DNS roots that aren't managed by the ICANN and have URLs with nonstandard top-level domains. Such sites usually require a specific DNS server to resolve their URL. Other examples are sites that registered their domain name on a completely different system than the standard DNS, like the .bit domains (Ciancaglini, Balduzzi, McArdle, and Rösler, 2015).

So Deep Web is that place on the World Wide Web which cannot be accessed via search engines' keyword search but can be reached by entering the exact destination URL in any conventional web browser. Although it is almost infeasible to accurately predict the size of this Invisible Web, it is estimated to be 400-500 times larger than the Surface Web. Since Deep Web content is not displayed to everyone in search engine results, this part of the Web offers a higher level of privacy as compared to Visible Web pages. However, Deep Web websites are still under the authority of Internet Service Providers that provide private server hosting services. While they ensure privacy, they are far from being anonymous (Norton, 2016). Anonymity on the Web is offered by a different segment of the Web, known as the Dark Web.

DARK WEB

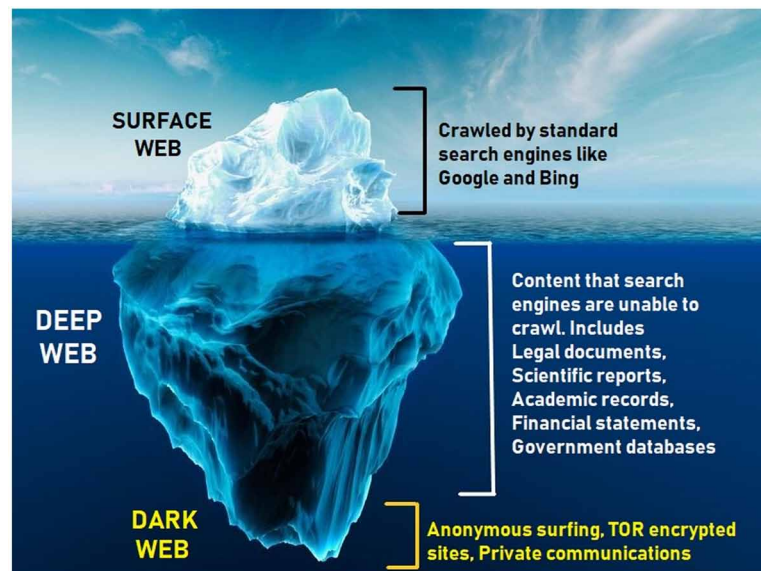
The segregation of the Web into Visible and Invisible Web has been caused by present-day search engines which can crawl only hyperlinked content. Though data on the Invisible Web remains hidden, this layer of the Web was never purposely created to conceal information. Rather, there exists another part

of the World Wide Web which was specifically developed with the aim of hiding every activity taking place on it. This is known as the Dark Web. Many people lack a clear understanding of these two layers of the Web: Dark Web and Deep Web. Some people assume Dark Web is same as the Deep Web, while others claim that these are two disjoint layers. Both these statements are incorrect. The Dark Web is a subset of the Deep Web. Like the Deep Web, Dark Web also remains unindexed by search engines but unlike Deep Web, it cannot be reached through standard web browsers. Dark Web requires specialized softwares, specific configurations and authorizations to be accessed (Dange, Malkan, and Jha, 2018). Figure 1 depicts these 3 layers of the World Wide Web in the form of an iceberg.

Another important difference includes the stability of websites/web pages hosted on Invisible Web and Dark Web. While sites on Surface Web and Deep Web are usually stable and stay up for long durations of time, websites on the Dark Web tend to have a shorter life span as compared to Clearnet websites. A survey of Dark Web was conducted by *Securelist* and it was found that most of the sites on this part of the Web are quite unstable. While most Dark websites were found to be active for a duration between 200-300 days, there were many sites that were only live for around 60 days (Intelliagg, 2016). Even with these characteristics, the popularity of the sites on the Dark Web has been on the rise.

Though the Dark Web has existed for years, one incident that brought it into limelight was the hacking of Ashley Madison database in 2015. Ashley Madison is an online dating platform for married people. During July 2015, hackers were able to access its database containing personal details of around 37 million customers. Around 9 GB of this data, including clients' names, addresses, emails, sexual preferences and credit card information, was dumped on Dark Web (Weimann, 2016). This incident drew major public attention and gave a boost to the popularity of this part of the World Wide Web. If we compare the World Wide Web to an ocean, the Visible Web are the waves present on the surface. Below the surface, lies the invisible world of the Deep Web. And the deepest part of this Invisible Web, requiring highly specific tools and equipment to reach, is the Dark Web. TOR is one such tool that opens the doors to the world of Dark Web.

Figure 1. Different parts of the World Wide Web are displayed as different portions of the iceberg



TOR: GATEWAY TO THE DARK WEB

Navigating websites on the Dark Web is becoming increasingly convenient as new software enter the markets every day. These software offer anonymising and encrypting facilities to access Dark Web websites. TOR is one such software that has been the most popular candidate in this category. TOR is an acronym for “The Onion Router”. It is a free software that allows anonymous communication over the Web. People often use the acronym TOR to refer to both the TOR network as well as the TOR browser. While the TOR network is a collection of a large number of volunteer computers that run a specific server application, the TOR browser allows users to hide their identities when accessing the content hosted on the TOR network (Poobalan, 2018). In essence, the TOR browser is used to access the TOR network. Its sole purpose is to conceal users’ browsing patterns, preferences, location as well as their actual identities in the Internet space. Thus TOR allows its users and their online activities to remain untraceable (Cooper and Chikada, 2015).

At present, TOR is a non-profit project which includes maintenance of the software as well as the network. It is run by people who actively strive for users’ right to online privacy and anonymity. Even with its expanding user base, TOR strives to remain non-profit and never collects user data (Poobalan, 2018). This has deepened the trust of its audience and made it famous in the Dark Web community. With a total of 17.5 million downloads recorded till date, the TOR project claims to have around 2 million daily users. Though most of these users find TOR services to be slower than connections made on the Surface Web, they are ready to pay this price for the services it offers. TOR’s slow speed is a result of its anonymizing technology, called Onion Routing. This technique was developed by the U.S Navy back in 1990s so as to safeguard its online intelligence communication (Poobalan, 2018).

To preserve user anonymity, TOR encrypts its traffic several times. This encrypted traffic is then directed through multiple TOR servers that are a part of the TOR network. These servers (sometimes referred to as relays/routers) are always selected randomly during connection establishment in order to create a private and secure communication pathway. At each relay node, one layer of encryption is removed so that the current node can discover the address of the next destination node. This is similar to peeling an onion, layer by layer, such that every relay can only peel the topmost layer. Hence the name the Onion Router. Onion Routing gives rise to an encrypted connection that is built step by step between every two nodes, such that each node only knows from which node it received data packets and to which node the received packets must be forwarded. This prevents tracing the source and destination of any user request. This way the TOR network allows its users to hide their online footprints and escape surveillance.

TOR is one way to enter and sail through the Dark Web. Other well-known alternatives include I2P (Invisible Internet Protocol) and Freenet. While I2P provides anonymity between applications via encrypted connections, Freenet utilises peer-to-peer facilities to establish a fresh path for every new connection. Though this makes reopening of pages slower, Freenet is considered simpler and more convenient by the end users. With many such anonymization software available online, it is becoming easier to be a visitor as well as a host on the Dark Web. This has allowed different kinds of users to access and host a variety of illegitimate and legitimate services on the Dark Web.

ILLEGITIMATE ACTIVITIES ON THE DARK WEB

1

The Dark Web allows its users to anonymously access its websites through the use of software like TOR. This way they are able to escape surveillance and their identities, preferences, locations and online activities also remain hidden. Though online anonymity paves way for user privacy, it also opens doors to a plethora of criminal activities. In recent times a large number of websites have come up on the Dark Web that provide illegitimate goods and services. Some of these are:

1. Counterfeit Currency

The Dark Web acts as the distributor of counterfeit currency which is sold with a guarantee of surpassing standard ultraviolet light checks successfully. Money to be paid in such cases varies with the quality, quantity and the type of currency being falsified. For example: Six hundred dollars can fetch around twenty five hundred dollars in counterfeit U.S. notes (Dange, Malkan, and Jha, 2018).

2. Forged Documents

Several sites on the Dark Web are also famous for providing fake passports, immigration papers, driving licences and other identity documents for any country in the world (Ciancaglini, Balduzzi, McArdle, and Rösler, 2015). The price of these documents mainly depends upon the country in which they will be used. These services allow notorious people to acquire fake citizenship as per their needs. Other forged documents that are readily available include citizenship papers, fake IDs, college diplomas and even diplomatic identity cards.

3. Drugs

Different types and quality of illicit drugs can be purchased on the Dark Web. Even banned drugs and pharmaceutical products like Ritalin and Xanax also find a place on Dark Web marketplaces (Ciancaglini, Balduzzi, McArdle, and Rösler, 2015). Silk Road is an example of a Dark Web marketplace which became famous for the wide range of drugs that were sold through it in huge amounts.

4. Stolen Confidential Information

This includes buying and selling of stolen credit card details, bank account details and even personal information like social security numbers. Apart from physical credit or debit cards, bank accounts can also be purchased at different prices in this Dark world.

5. Hackers

Another community that benefits from the Dark Web, includes hackers. They can easily buy sophisticated malwares and even get paid by interested parties to carry out any kind of online hacking attacks against specific governments, organisations or individuals (Spalevic and Ilic, 2017).

6. Arms and Ammunitions

Illegal trade of explosives, weapons and firearms is also carried out openly. These services ensure that the requested goods are delivered to the buyer in special packaging that can easily cross any kind of scanning and security checks. Sometimes, arms and ammunitions are stuffed in children's toys or electrical equipment to evade the eyes of authorities (Dange, Malkan, and Jha, 2018).

7. Hitmen

Many portals on the Dark Web allow people to hire professional assassins. Often the hiring party has the option of specifying how they want their enemy/opponent to be murdered – using regular methods or through bombing, torture, rape etc. Money demanded for such acts varies with the selected murder method and the social status of the victim (Spalevic and Ilic, 2017).

8. Human Organ Trafficking

Human organ trafficking is another business which has its roots deeply penetrated in the Dark Web. Kidneys, liver, heart and eyeballs are examples of frequently bought organs in these black markets (Dange, Malkan, and Jha, 2018).

9. Terrorist Activities

The anonymity of this part of the Web has given a huge boost to major terrorist groups across the world. From secret communication and propaganda to recruitment and training, everything that cannot be openly done on the Visible Web, is carried out through Dark Web (Sui, Caverlee, and Rudesill, 2015) ; (Weimann, 2016).

10. Child Pornography

The Dark Web has also become a famous destination for hosting child abuse videos as well as child pornography. Though the Visible Web also faces the problem of illegal hosting of such videos, but this problem is much graver in this dark underground world. In 2012, the Federal Bureau of Investigation (FBI) launched “Operation Torpedo” against the users of three Dark Web websites that hosted child pornographic videos (Sui, Caverlee, and Rudesill, 2015). This highlights the intensity of this problem.

The list of illicit activities carried out using Dark Web is endless. Criminals thrive in this secret world because procedures to trace their footprints are complex and tracking them is next to impossible. A key factor responsible for the growth of Dark Web based crimes is the use of Bitcoin like cryptocurrencies as a mode of payment.

USE OF BITCOIN ON DARK WEB PLATFORMS

Cryptocurrencies are digital currencies that are secured using cryptography methods. Most financial transactions on the Dark Web are carried out through digital currencies like Bitcoin. This is a preferable method of payment because cryptocurrencies ensure the anonymity of the transaction – not only

the amount of money exchanged but also the identities of the involved parties. Together with browsers like TOR and I2P, cryptocurrencies offer a dual layer of obscurity to the Dark Web domain. This allows notorious people to trade Bitcoins for anything they want on the Dark Web without getting noticed by the legal authorities. Users who wish to trade through Bitcoin, must maintain a Bitcoin wallet (called the dark wallet when used on Dark Web) either on their own or through third parties (Piazza, 2016). There is also a provision of obtaining special credit cards if the Bitcoin wallet owner wants to cash his Bitcoins. The websites offering such cards assure its users that the source of their transactions shall remain masked. Many websites on the Dark Web use Bitcoin as the sole medium of transaction. Silk Road was an example of one such site.

SILK ROAD

Silk Road was an online marketplace on the Dark Web. It was developed, owned and operated by a young programmer named Ross William Ulbricht. To hide his actual identity, Ross operated with the administrator name “Dread Pirate Roberts”. Silk Road started its operations in 2011 and carved a niche for itself with its highly professional website. In a small period of 3 years, the popularity of this site went up as more and more drugs were listed and made available through it (Bhaskar, Linacre, and Machin, 2017). Services like computer hacking, selling of forged passports, driver’s licences, credit cards and identity documents like Social Security Numbers were also provided on this platform. Apart from this, the website also hosted a community forum that offered suggestions on how to avoid the eyes of law enforcement by transacting safely on the platform. Silk Road, which was accessible only through the TOR network, accepted its payment only in Bitcoins. In the time period between February 2011 and July 2013, around 1.2 million transactions were recorded on this website from almost 3,877 unique seller accounts and 147,000 unique buyer accounts. This helped Ulbricht to build a massive empire worth \$ 1.2 billion in such a limited time. In one of the interviews given by Ulbricht to Forbes magazine, he claimed that he would never be caught. But Silk Road’s journey concluded with the arrest of Ulbricht inside the San Francisco Public Library followed by shut down of Silk Road in 2013 (Poobalan, 2018). Ulbricht was found guilty and received life imprisonment without any chance of parole. The severity of this punishment was due to charges against him that included money laundering, computer hacking and conspiracy to traffic narcotics through internet. Ulbricht’s case made headlines and led to a boost in the popularity of the Dark Web among common people. A month after Ulbricht’s arrest and shutdown of Silk Road, it was started again by Blake Benthall. This time the business boomed for a year, before its owner Blake Benthall was arrested and the website was shut down again. An hour later the portal was revived again. Just like its predecessors, Silk Road 3.0 is like any normal e-commerce platform but with “not-so-normal” listings.

According to (Dange, Malkan, and Jha, 2018) the value of Bitcoin was directly affected by the growth of Silk Road. Bitcoin tripled in value just a month after Ulbricht founded Silk Road. This sudden hike in price drew attention of investigators and as they started exploring the causes, Bitcoin lost about 90% of its value. Though Silk Road was eventually shut down, but this was not an easy task for law enforcement authorities. One factor that added to its difficulty was the use of Bitcoins for conducting transactions. The use of digital currencies did not remain limited to Silk Road. Most black markets now use Bitcoin as a preferred mode of payment. To deal with this upsurge in Bitcoin financed cyber crimes, law enforcement authorities have started taking strict actions against the owners/administrators of many famous Dark web portals.

CURBING CRIME ON DARK WEB

As cyber criminals devise new ways to exploit the anonymity offered by the Dark Web, law enforcement agencies across the globe are also developing new strategies to deal with them. Although Bitcoin and TOR wrap the world of Dark Web in double layers of anonymity, but these layers are just as strong as their weakest point. Even if Bitcoin transactions do not carry any personally identifiable information, there are several other ways of nabbing Dark Web criminals. For instance, drugs purchased online are eventually delivered to a geographic location via the postal system. This can give a major lead to the investigators who aim to catch potential suspects. Another activity that quickly draws the attention of law enforcement, is the conversion of large amounts of Bitcoin to fiat currency. An example of this was a police raid in Netherlands that led to the arrest of ten men who were caught encashing Bitcoins and withdrawing millions from ATMs (Bohannon, 2016).

But incidents like these do not happen often, so law enforcement agencies along with the research community has started focusing its attention towards analysing the patterns of Bitcoin transactions to uncover notorious participants of Dark Web platforms. Continuous monitoring and data collection of Dark Web's transactions can help to identify Bitcoin addresses that belong to the same person/group if they are used as input in the same transaction. In (Reid and Harrigan, 2013) the authors proposed to use Directed Acyclic Graphs to represent the flow of Bitcoins between users and transactions to highlight interesting patterns of user activity. Clustering algorithms based on unsupervised machine learning can also help to isolate Bitcoin addresses with multiple incoming transactions as belonging to online vendors hidden in the Dark Web marketplace. In addition to this, if investigators get access to suspected Bitcoin wallets, important information about the owner's identity and past transactions can be easily revealed through the associated "wallet.dat" file (Turner and Irwin, 2018).

Though analyses of Bitcoin addresses can expose significant information, but generally multiple addresses are linked to each wallet and Bitcoin owners tend to use different addresses for each transaction to increase anonymity. This is a severe obstruction while clustering Bitcoin transactions and tying them to physical identities. To increase the problem, Bitcoin mixing services are also offered on the Dark Web that aim to break the money trail and weaken the link between transactions and Bitcoin wallet owners (Wegberg, Oerlemans, and Deventer, 2018). So investigators have now shifted their attention towards methods that map Dark Web's financial transactions to their source and destination IP addresses. In an effort to establish such a mapping, Philip and Diana Koshy developed software similar to the one used by Bitcoin vendors and buyers to interact with Bitcoin blockchain. The financial transactions of everyone interacting through this software was accessible by the Koshys. The couple noticed patterns in the number of transactions being sent out by certain IP addresses and were able to map around 1000 Bitcoin addresses to their corresponding IP addresses (Bohannon, 2016). Such IP tracing methods offer significant advantage in de-anonymising cyber criminals that mask behind Dark Web and can be seen as a first step towards breaking the anonymity offered by TOR. But many times even these techniques are not enough.

Sometimes the investigators themselves have to get their hands dirty to clean the Dark Web. There have been instances when law enforcement personal had to pose as vendors/buyers of illegal weapons and drugs on Dark platforms in order to entice cyber criminal and catch them in the act. When such tactics failed to meet their purpose, investigators have to level up their game by using "network investigative techniques" to catch suspects. This surveillance method remotely installs malware on a suspect's computer and helps investigators to follow the suspect's activities on the Dark Web without accessing his/her device physically (Ghappour, 2017). The level of anonymity that Dark Web has developed, is not

easy to infiltrate and there have been instances where cyber criminals who have been caught by their own negligence. It was Robert Ulbricht communication on a public forum where he advertised Silk Road, that eventually busted him (Ghappour, 2017). After all, to err is human! Though law enforcement tries its best to curb the use of Dark Web, there exists a legitimate side to this world as well.

LEGITIMATE USES OF THE DARK WEB

There is no doubt that the Dark Web has become a hotbed of cybercrime that is funded by cryptocurrencies. But originally it was not developed for this purpose. There were noble intentions behind its development. And even today, there are many Dark Web users who are not involved in any illicit activity and use this Web for legit purposes. These people utilise the anonymity of the Dark Web to bring about a positive change. Common examples include:

- People living in countries under suppressive regulations, often use the anonymity of the Dark Web to convey their ideas and thoughts. Revolutionary ideas in such regions are often toned down and that's why individuals or even groups try to communicate with public through Dark Web platforms. For example, Facebook launched a version of its website on TOR network to provide its services to users who live in countries that ban the use of Facebook. This version which can be accessed at <https://facebookcorewwi.onion/> allows people to communicate with each other at higher levels of protection against surveillance.
- Journalists and whistleblowers also utilise the Dark Web to reveal information that should be brought to the notice of the common man, but remains veiled. They use the Dark Web to anonymously highlight important information and incidents without fearing political surveillance and suppression. In 2010, TOR was given an award for Projects of Social Benefit from the Free Software Foundation for helping whistleblowers and supporters of human rights (Sui, Caverlee, and Rudesill, 2015).
- Bloggers, writers and other creative people who fear censorship on the Surface Web, become frequent users of the Dark Web.
- Celebrities and common people who do not want to leave behind any kind of online trail including their identity, search history or location, are active users of the Dark Web.
- Researchers, students and teachers who want to access vast resources of knowledge available on the Dark Web, also access this part of the Web for legitimate purpose. Many scientific findings that have not been made public on the Surface Web, can be easily found on the Dark Web (Dange, Malkan, and Jha, 2018).

Such people look upon Dark Web as a haven that offers anonymity, freedom of speech and privacy. Though this aspect of Dark Web is rarely highlighted, this was the sole reason behind its development.

CONCLUSION

The Dark Web is that part of the World Wide Web which is neither crawled by conventional search engines nor accessible through traditional web browsers via URLs. It requires the use of specific software and configurations to enter and sail through this part of the Web. A lot of time and patience is also

needed to explore the Dark Web content. But users tend to pay this price in exchange of their privacy in this digital underground world. This need for privacy draws the attention of people who do not want to be tracked while surfing the Web but cannot find a way for the same on the Surface Web. The Dark Web looks like a lucrative option to them. But Dark Web's anonymity is a double edged sword – it all depends how one uses it. People who seek online anonymity come from different corners of the world, with different intentions in their mind. When used in a benevolent manner, Dark Web can serve as a medium to ensure user's online privacy. But with malevolent intentions, it can become a playground for criminals. Therefore, like every other invention, the Dark Web has its own set of pros and cons. It can prove to be very useful or disastrous depending upon its application. The manner in which it is utilised, ultimately decides whether Dark Web is a boon or a bane.

REFERENCES

- Balduzzi, M., & Ciancaglini, V. (2015). *Cybercrime in the Deep Web Black Hat EU*. Amsterdam: Trend Micro.
- Bhaskar, V., Linacre, R., & Machin, S. (2017, November 6). *Dark web: The economics of online drugs markets*. Retrieved from LSE Business Review: <http://blogs.lse.ac.uk/businessreview/2017/11/06/dark-web-the-economics-of-online-drugs-markets/>
- Bohannon, J. (2016, March 9). Why criminals can't hide behind Bitcoin. *Science*. doi:10.1126/science.aaf4167
- Ciancaglini, V., Balduzzi, M., McArdle, R., & Rösler, M. (2015). *Below the Surface: Exploring the deep Web*. Trend Micro. Retrieved November 28, 2018, from https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf
- Cooper, E., & Chikada, A. (2015). *The Deep Web, the Darknet, and Bitcoin*. MarkMonitor - Part of Thomson Reuters. Retrieved November 28, 2018, from <https://www.markmonitor.com/download/webinar/2015/MarkMonitor-Webinar-150715-DeepWebDarknetBitcoin.pdf>
- Dange, V. R., Malkan, K., & Jha, M. (2018). *Monograph on Dark Web*. Dhole Patil College of Engineering, Department of Computer Engineering. Pune. Pune: Dhole Patil College of Engineering.
- Ghappour, A. (2017). Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. *Stanford Law Review*, 69, 1075–1136. Retrieved from https://repository.uchastings.edu/faculty_scholarship/1583
- Intelliagg. (2016). *Deeplight: Shining A Light On The Dark Web*. London: Intelliagg.
- International Telecommunications Union. (n.d.). Retrieved November 28, 2018, from [https://media.scmagazine.com/documents/224/deeplight_\(1\)_55856.pdf](https://media.scmagazine.com/documents/224/deeplight_(1)_55856.pdf)
- Norton, J. (2016). *TOR and The Dark Net Learn To Avoid NSA Spying And Become Anonymous Online*. Createspace Independent Publishers. Retrieved November 28, 2018, from http://mirror.thelifeofkenneth.com/lib/electronics_archive/TorAndTheDarkNet-JaredNorton.pdf
- Piazza, F. (2016). Bitcoin in the dark web: A shadow over banking secrecy and a call for global response. *Southern California Interdisciplinary Law Journal*, 26, 521–546.

Poobalan, D. (2018, June 15). *The Dark Web: Myths, Mysteries and Misconceptions*. Retrieved November 28, 2018, from <https://go.kaspersky.com/rs/802-IJN-240/images/Dark%20Web%2010172017.pdf?aliId=521973948>

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197–223). New York: Springer. doi:10.1007/978-1-4614-4139-7_10

Santos, N. (2015). *Deep Web*. Tecnico Lisboa. Retrieved November 28, 2018, from <https://fenix.tecnico.ulisboa.pt/downloadFile/563568428719095/csf-18.pdf>

Spalevic, Z., & Ilic, M. (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika (Nis)*, 63(1), 73–82. doi:10.5937/ekonomika1701073S

Sui, D., Caverlee, J., & Rudesill, D. (2015). *The Deep Web and Darknet: A look inside the internet's massive black box*. Academic Press.

Turner, A., & Irwin, A. S. (2018). Bitcoin transactions: A digital discovery of illicit activity on the blockchain. *Journal of Financial Crime*, 25(1), 109–130. doi:10.1108/JFC-12-2016-0078

Wegberg, R. v., Oerlemans, J.-J., & Deventer, O. v. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419–435. doi:10.1108/JFC-11-2016-0067

Weimann, G. (2016). Going dark: Terrorism on the dark Web. *Studies in Conflict and Terrorism*, 39(3), 195–206. doi:10.1080/1057610X.2015.1119546

ADDITIONAL READING

Amores, R. G., & Paganini, P. (2012). *The Deep Dark Web: The Hidden World*. CreateSpace Independent Publishing Platform.

Bartlett, J. (2014). *The Dark Net: Inside the Digital Underworld*. London: William Heinemann.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in future. *Journal of Policing, Intelligence and Counter Terrorism*, 13(3), 285–300. doi:10.1080/18335330.2018.1506149

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital ‘demimonde’. *Information Communication and Society*, 19(1), 111–126. doi:10.1080/1369118X.2015.1093531

Masterson, S. (2015). *Tor Browser Handbook: Quick Start Guide On How To Access The Deep Web, Hide Your IP Address and Ensure Internet Privacy*. Advanced Tech Guides.

Ormsby, E. (2018). *Darkest Web: Drugs, death and destroyed lives ... the inside story of the internet's evil twin*. Australia: Allen and Unwin.

Tomažič, T., & Vilela, N. B. (2017). Ongoing Criminal Activities in Cyberspace: From the Protection of Minors to the Deep Web. *Revija za kriminalistiko in kriminologijo/Ljubljana*, 68(4), 412–423.

KEY TERMS AND DEFINITIONS

Bitcoin: It is a kind of digital cryptocurrency that is used for transactions in many black markets of the dark web.

Crawling: It is the process by which search engines gather online information through crawling robots by moving from one web page to another by the use of hyperlinks.

Dark Web: The part of world wide web that allows its users to remain anonymous by the use of specialised software to mask their online presence.

Deep Web: The part of the world wide web that cannot be crawled by web crawlers and does not appear in results displayed by search engines.

Indexing: The process followed by search engines to create an index of the contents present on the Internet, to allow easy retrieval when displaying results to user queries.

Internet: It consists of networks across the world, interconnected together to form one massive global network.

The Onion Router (TOR): It is a free and open source software that allows anonymous communication over the dark web.

Surface Web: It is the part of the world wide web that can be easily accessed by everyone through the use of standard web browsers and search engines. It is also known as clearnet or visible web.

World Wide Web (WWW): It provides information sharing capability to the Internet through web pages that are hosted online using hyper text transfer protocol (HTTP).

File-Sharing and the Darknet

1

Martin Steinebach

 <https://orcid.org/0000-0002-0240-0388>

Fraunhofer SIT, Germany

INTRODUCTION

The public interest in free information exchange is considerable. Besides textual information, this includes multimedia content, data sets and software as well. Compared to text data, the latter require the transfer of huge data volumes, which cannot be handled via Email, forums or chats. In part, the Internet is also rooted in this interest. (Nelson et al., 1981) addressed the global exchange of research results as early as 1960 in the Xanadu project.

However, the free exchange of information can also be misused for illegal measures, including copyright violations, the distribution of child pornography, illegal propaganda or instructions for building explosives. The degree of stigmatization for these use cases varies largely. Large parts of the Internet community has always supported the uncontrolled distribution of copyrighted material. This has led to a constant battle between copyright holders and file sharing activists, with technological advances on both sides. The automated crawling of IP addresses by file sharing peers was answered by obfuscation measures, which can be seen as first approaches to privacy networks. Legal discussions about the impact of file sharing for copyrights were initiated as well (Wood, 2009).

These networks allowed distributing arbitrary file types, often arguing with privacy and the risk of censorship in more public file distribution networks and mentioning documents with political backgrounds as the typical data to be shared. However, they were also utilized for the file sharing of mp3s and movies. Child pornography is reported to be commonly shared via such protected networks as well.

Privacy networks and the file sharing in it are typical examples of a dual use, but this work will not be discussing the pros and cons. Every side will find arguments either for supporting or prohibiting this technology. In addition, the legal aspects of file sharing and copyright differ depending on the country. Our aim is to show which role file sharing and the growing need for privacy within it played in the development of privacy networks and how to achieve privacy in file sharing networks today.

BACKGROUND

With increasing download speeds and the general growth of the Internet, sharing content over the Internet became more and more common. Even before the world wide web was introduced, mailing lists and FTP servers were used to access illegal copies of photos, documents or (with the rise of mp3) songs. The first file sharing methods were still centralized and depended on a server. Law enforcement or administrators could easily attack these servers. This led to the adoption of alternative infrastructures, the peer-to-peer networks. File sharing via peer-to-peer networks has been used for the exchange and distribution of copyrighted material since the advance of this technology.

DOI: 10.4018/978-1-5225-9715-5.ch011

This section discusses the history of illegal content distributed via the Internet, commonly called 'warez', and first general approaches to distributed warez without being monitored and sued.

Bulletin Boards

The concept of warez existed even before the Internet as we know it today. The book NO COPY reports from the origins of today's warez scene (Kroemer & Sen, 2006). In the 80's copyrighted contents were distributed in so-called Bulletin Board Systems (short: BBS). The dial-in into these forums was not as common as today and typically only technically interested people met there.

In these small communities, it was important that members actively supported the community before downloading, for example by uploading their own content or commercial software with removed copy protection. Commercial interests were almost not existent. At the end of the 1990s, the law enforcement took stronger action against this community.

This led to uncertainty among many participants, who now regarded the support of the scene as too great a personal risk. At the same time, the Internet, as we know it today, began to gain popularity. As a result, many warez from the BBS were uploaded and made accessible to everyone. These two factors were mainly responsible for the decline of the Bulletin Boards.

World Wide Web

Various, mostly commercially motivated ways of obtaining illegal copies of media have developed to this day on the Internet. Sites like Kinox.to or Bs.to provide hyperlinks to movies and series freely. According to an estimate of the Alexa.com website, these two were the 36th and the 23rd most visited websites respectively (Alexa, 2016). The small communities of the 1980s and 1990s, which in their time had made only little access to copies possible, have now been replaced by websites with millions of clicks. Everyone with an Internet connection can access them, and banners and similar advertisements monetize this massive access. According to the Motion Picture Association of America (MPAA), today's warez scene is pyramid-like structured (MPAA, 2006). The so-called suppliers procure the material, for example by filming cinema performances, and sell these recordings to replicators and release groups. They multiply the material explosively and make it available to other people, the facilitators. They download the content from the servers of the release groups, which are also called top sites, and upload it to publicly accessible sites. Once this has been done, the masses can access many different offers to access the illegal material. In this way, a few sources supply the entire Internet with warez. A more detailed view on the warez scene can be found in the article by D'ecary-H'etu et al. (D'ecary-H'etu, Morselli, & Leman-Langlois, 2012).

Peer-to-Peer Networks

A peer-to-peer (P2P) network describes a network architecture in which all network participants have equal rights. Unlike a client-server infrastructure in which clear roles are assigned, nodes in a P2P network can both provide and retrieve services. Most P2P networks use the infrastructure of the Internet as a basis and are organized centrally or decentrally depending on the implementation[25]. Since early P2P networks allowed a simple identification of peers, for example by their IP address or similar identifiers,

many approaches for monitoring have been documented. Some are more general (Banerjee, Faloutsos, & Bhuyan, 2007) and include legal discussions (Smith, 2003). Others aim at specific protocols. Chotia et al. address BitTorrent monitoring (T. Chothia, Cova, Novakovic, & Toro, 2012), Yang et al. (Yang, Ma, Song, Cui, & Zhou, 2006) discuss monitoring eMule, Saroiu et al. (Saroiu, Gummadi, & Gribble, 2003a) address Napster and Gnutella.

Private peer-to-peer networks extend P2P networks by various access restriction mechanisms like the allocation of passwords or keys. In a more special version of a private P2P network, the so-called Friend-to-Friend-Network (F2F), exactly these possibilities are used. With F2F networks, it is also not possible to register participants of the network outside their own friends list. These strategies obfuscate the activities within a file sharing network. An investigator cannot directly approach participants and scan for offered illegal files. He needs to get the trust of users and become a member of the network.

One of the best-known P2P networks still in use today is BitTorrent. The BitTorrent protocol is a decentralized structure for distributing data between users, the peers (Cohen, 2003). A central server, also called a tracker, keeps track of all peers who want to download a file. When a new peer connects to the tracker, it gets the addresses of some other peers who have already downloaded the file or are still downloading it. The peer will now begin to download the file, divided into small pieces, from several other peers. So the individual users, not dedicated servers, provide the bandwidth here. Since the different peers have a direct connection with each other, criminal prosecution of the different participants is possible without great effort (T. Chothia et al., 2012), if they do not protect themselves with VPNs or the like. It has also been shown that in some cases this prosecution is erratic (Piatek, Kohno, & Krishnamurthy, 2008).

The Usenet

The Usenet is a decentralized network where users exchange messages via "news servers". It consists of many servers that connect to each other and exchange messages. It can be seen as a direct successor of the already mentioned bulletin boards. To participate in the message exchange, users need a newsreader, which displays the postings from one of the Usenet servers. Through this newsreader, the user can also reply to messages and open new threads. The messages are then sent to the news server, which forwards them to all servers connected to it. Other users can retrieve this message even if they are connected to another news server. Messages are sorted in subhierarchies. Copies of software and other media are mainly exchanged in the alt.binaries subhierarchy (Anonym, n.d.), which is further subdivided for the different media types. Since these subhierarchies cause a lot of traffic, they are usually only offered by commercial news servers that require a monthly usage fee. The data exchange is encrypted and not logged, it is therefore very difficult to prosecute the individual users. However, there are ways to remove copyrighted material from the Usenet. A complete prevention of illegal data exchange is difficult due to the decentralized nature of the Usenet.

Private FTP servers

Small groups who want to exchange data usually do so via FTP servers. These privately operated servers are usually rented abroad with fake address data. Criminal prosecution is virtually impossible if the servers are configured correctly: access is only indirect, encrypted and not logged. This is coupled with the fact that only a few people even know about the existence of such a server.

Sharehoster

Sharehosters, also called one-click hosters or cyber-lockers, allow users to upload and download files on dedicated servers. Downloading files is only possible if the user knows the link to a file. This link usually consists of a pseudo-random sequence. These links are usually exchanged over external pages. As the servers operate in countries with less strict copyright laws, it is difficult to track individual downloaders due to limited legal support. Antoniadou et al. discuss this in more detail in (Antoniades, Markatos, & Dovrolis, 2009). The most popular case may be Megaupload, a sharehoster that paid for uploading content and became subject of a massive criminal investigation leading to its shutdown (Kang, 2012).

Obfuscation Strategies

Independent of the strategy actually used for obtaining warez, the IP address is visible to the downloading party at the point where the file exchange from one user to another occurs and may therefore potentially reveal the identity of the other peer:

the IP address is matched to the user by the respective Internet provider.

An obvious and effective method of obfuscating one's own identity is the use of public accesses without the need of authentication. The IP address in this case only leads to the public access, but not the actual user. However, it requires visiting a public access device and is usually subject to limited Internet speed.

The use of a Virtual Private Network (VPN) is logistically less demanding. The actual purpose of a VPN is the private communication with devices in a locally limited and shielded network, such as the intranet of a company, without being physically present there. A VPN opens a tunnel from the user to a service provider. When accessing the Internet via VPN, the user appears to come from the country of the VPN server and uses the IP address range of the provider.

The effect is similar to the use of a seedbox. Here, the user rents a virtual or physical machine from a third party on which he runs his file sharing client. Periodically, the user connects directly to the seedbox to download the accumulated files and issues new commands.

In both cases, the protection of the user's identity is the responsibility of the service provider, either the VPN provider or the host of the seedbox. The improvement of privacy depends on the service providers. China's "Great Firewall" is an example of censorship efforts that were initially bypassed by using VPNs and are increasingly accompanied by technical and political measures to suppress various evasion strategies.

PRIVACY-ENABLED FILE SHARING

Privacy mechanisms have been added to file sharing networks over the last 20 years. This section provides an overview of several approaches. They can be seen as an evolution of privacy away from early networks like Napster or Gnutella (Saroiu, Gummadi, & Gribble, 2003b) (Bellovin, 2001) or as a natural reaction to the file sharing monitoring (F.-S. T. Chothia, Chothia, & Chatzikokolakis, n.d.).

Beyond the technology we describe below, other file sharing networks have been developed claiming to provide user privacy. Among them are GNUnet, open source solutions RetroShare, OFFSystem and MUTE, as well as closed source Zultrax, Proxyshare, Nodezilla, Share and Winny. Most of them are of minor importance and are no longer in development.

Freenet

1

The freenet network (Clarke, Sandberg, Wiley, & Hong, 2001) basically treats all content as distributed files and allows the storage and exchange of large files. In combination with distributed storage, an overlay network, through which search queries and file transfers are routed, protects the identity of users. However, freenet's transfer rate is comparatively low, making it unattractive for exchanging large files. Freenet makes it possible to make the provision and acquisition of information anonymous by presenting itself as a decentralized data store that enables access to information anonymously with the help of encryption and clever routing. The freenet network must not be confused with Freenet.de, the access provider of the same name. The manner in which this is implemented in Freenet will be explained in the following.

Freenet consists of a number of equal computers (nodes) which are operated by individual users. Each node performs client and server tasks simultaneously. In addition, when installing the freenet software, each node releases storage space on its computer for use by freenet, in which both it and all other freenet nodes store, read, and forward content. The user defines the maximum size of this data store. Access to this encrypted data container is managed by the freenet clients. Once a file has been released, it cannot easily be removed from freenet access by the user. All these nodes and their associated data stores together form the freenet network. The content of each node's data store is encrypted. The user therefore does not know which data is currently on his disk or which information he is forwarding.

The transfer between the nodes also takes place in encrypted form, so the users cannot see which information is passing through the freenet via their computer. The freenet is therefore primarily a large, encrypted, anonymous file system with encrypted protocol information and not a file sharing protocol in the narrower sense. This is also a big difference in networks like Napster or Gnutella. With these networks, users make resources available that are located on their computers. These resources are available as long as the computer is connected to the network. Gnutella does allow a certain file to be redundant because it is stored by several users at the same time. After disconnecting all these users, however, the resource is no longer available.

In the freenet network, on the other hand, resources that are frequently requested are implicitly redundant in the network and move from node to node and are therefore available, regardless of whether the originator of the resource is connected to the network or not. Redundancy is therefore implicitly linked to the freenet protocol, regardless of user behavior.

This in turn means that freenet cannot guarantee that any specific information will be available forever. Because the number of computers involved limits the storage space, old information may be replaced by new information if the latter is frequently requested. However, it can be assumed that freenet's easy extensibility will always provide enough storage space for the information, as each new user also integrates new storage space into the network.

I2P

I2P (Astolfi, Kroese, & van Oorschot, 2015) is a software published under several free licenses, which allows the construction of an anonymous network. It has parallels to TOR and freenet. Similar to freenet, it is a decentralized darknet that stores routing information in a distributed manner. Routing, on the other hand, is an extended form of onion routing used by TOR and is called garlic routing. Similar to onion routing, the traffic is encrypted layer by layer. In addition, several requests are bundled into one packet and provided with an additional encryption layer (Schimmer, 2009). This also creates the analogy of

a garlic bulb. Another anonymization measure is the use of unidirectional tunnels, which means that requests and responses take different paths through the network. A tunnel corresponds to an encrypted connection in one direction between the sender of an inquiry and the processor, where other network nodes can also be crossed (Schimmer, 2009). This forwarding has the same effect as freenet, because it is no longer possible to trace whether a node has made or forwarded a request. The use of such unidirectional tunnels, however, increases the probability to pass an attacker's node within the network (Egger, Schlumberger, Kruegel, & Vigna, 2013). Addressing in I2P is based on Decentralized Hash Tables (DHT), so no directory servers are required as in the case of the TOR network. These tables contain information necessary to reach a specific endpoint within the I2P network. I2P offers the possibility to access the public Internet via an outproxy, but is not recommended because it is only about individual proxy servers. In addition, it provides web pages, so-called eapsites, and applications for sending anonymous mail, for example, but these are only internal to the network.

Tor

Tor is an acronym that stands for “The onion router”. It is an overlay network on the Internet that aims to protect the anonymity of its users (Syverson, Dingledine, & Mathewson, 2004). To achieve this goal all Internet traffic is encrypted using public and session key cryptography and sent through a network of several thousand relay nodes worldwide. Those relay nodes are hosted by volunteers who want to contribute to the network. To protect the anonymity of Tor users from attackers outside of the network all Internet traffic is encrypted and sent through the network on a predefined path using several relay nodes. This way an accessed website can only see the last IP address on the path through the Tor-network but not the originating IP address.

To protect against attackers inside the network the sent data is encrypted not only once but several times using public key cryptography. The name “The onion router” derives from this encryption because it is structured in several layers like an onion. Each of these layers of encryption can be decrypted by one of the nodes on the data's path through the network. If a node receives a data package, it decrypts the first layer of it to retrieve the data package with one less layer of encryption and an IP address to send it to. This way only the node where the data enters the network knows the originating IP address and only the node where it leaves the network knows the data's destination. Furthermore, if used correctly, none of the nodes knows the content of the data. In addition to anonymity enhancing options, Tor offers the possibility to host hidden services. Those are websites that can only be found within the Tor network. Due to the popularity of Tor these servers form a structure for which the term “darknet” is regularly used. Thereby they have become a synonym for the darknet.

Masking BitTorrent

BitTorrent (Pouwelse, Garbacki, Epema, & Sips, 2005) does not natively support measures to disguise user identity, but there is the possibility of private torrents. For these, a central tracker maintains a whitelist, and only passes information required for participation to trusted peers. Since BitTorrent also supports finding torrents using distributed hash tables, these private torrents depend on clients not overriding the appropriate flag in the torrent metadata.

BitTorrent via Tor: In this scenario, the user disguises his identity by using the Tor network as a proxy. Tor's network topology strictly differentiates between clients, nodes, and exit nodes, so the capacity of the network does not scale directly with the number of participants. Because file sharing requires a lot

of bandwidth (McCoy, Bauer, Grunwald, Kohno, & Sicker, 2008), Tor's network operators explicitly reject this application. Although the Tor network reduces performance, data exchange is faster than over freenet. However, the lack of official support increases the risk of misconfiguration and unwanted program behavior: For example, some BitTorrent clients transmit their own IP address assuming that the peers know it anyway.

BitTorrent via I2P: Unlike Tor, I2P supports both the UDP protocol and a number of ported BitTorrent clients, including the integrated I2PSnark client. Torrents that use the I2P network are isolated from torrents in Clearnet. Some clients can act as a bridge between the Clearnet and the I2P network by offering torrents in both environments. The owners of these bridges do not protect the privacy network.

OneSwarm

OneSwarm (Isdal, Piatek, Krishnamurthy, & Anderson, 2011) is a file sharing client that was initially released in 2009 and maintained until 2011. OneSwarm allows file sharing as a classic BitTorrent client, in a circle of confidants or through an independent overlay network that disguises the identities of the participants. This last operating mode promised significantly better performance than freenet and BitTorrent via Tor. It has been the subject of forensic investigations (Prusty, Levine, & Liberatore, 2011) aiming at identifying clients using it for sharing child porn.

The public part of a 1024-bit RSA key serves as a permanent pseudonym. Familiars can be added manually, using external means of communication such as email, or as a centrally managed group. In addition, public servers mediate peers not trustworthy (all peers who have not been explicitly trusted are not considered trustworthy). In the network, messages to these peers are randomly delayed or dropped altogether to prevent conclusions about neighboring nodes.

Since the network can only receive data that was previously sent, it is necessary to encourage peers to participate in the network. To this end, the amount of data received and sent by each immediate peer is compared. If a peer receives significantly more data than it sends, its priority drops during peak periods. Peers with extreme discrepancies are completely excluded.

RELATED WORK

Already in 2002, Biddle et al. mention the lack of anonymity in then popular file sharing networks and point to solutions like freenet (Biddle, England, Peinado, & Willman, 2003). They call any content distribution network darknet, which satisfies a number of requirements, but anonymity or privacy are not among them.

In 2003, the numerous lawsuits regarding warez traded on the Internet via various channels were summarized and discussed by Goldman in (Goldman, 2003). It provides a good overview on the viewpoint of criminal actions connected to warez.

In 2010, Chaabane et al. (Chaabane, Manils, & Kaafar, 2010) found that roughly 25% of Tor traffic was used for BitTorrent file sharing. They were also able to attribute individual file names shared and showed that new video games, movies and series to be the most frequently shared content over the combination of BitTorrent and Tor. The work by Zhang et al (Zhang, Dhungel, Wu, Liu, & Ross, 2010) on private BitTorrent sites from 2010 found that there were roughly twice as much public torrent sites as there were private ones.

Le Blond et al. (Blond et al., 2011) in 2011 discuss attacks able to trace BitTorrent streams on Tor by controlling a Tor exit node and monitoring outgoing traffic. This is possible as 70% of the users only connect to the BitTorrent trackers via Tor and share content unprotected. They provide various insights on the usage of file sharing via Tor. In their samples, the most popular content was shown to be pornography.

A more detailed analysis for content shared via I2P (masking both Gnutella and BitTorrent) and freenet is provided by Aked (Aked, 2011) in 2011. Child pornography was claimed to make up more than 50% of the content shared via freenet in this investigation. In I2P, the presence of child pornography was minimal. Movies, pornography and TV shows were the most prominent content here.

In 2013, Li et al. (Li, Erdin, Gunes, Bebis, & Shipley, 2013) published an overview of anonymity technology usage where also Tor and I2P are mentioned. They identified 61,798 Tor relays and 2,267 I2P relays. But they also found out in an experiment, that only very few peer-to-peer users utilized privacy protection: of sampled 128,422 IP addresses of peer-to-peer users, only 58 used a privacy mechanism like Tor.

A study from 2014 (Biryukov, Pustogarov, Thill, & Weinmann, 2014) analyzes 3050 hidden services with respect to their content. Here only 7% addressed software downloads.

In 2016, the European Union Intellectual Property Office (EUIPO) published a report (Deloitte, 2016) executed by Deloitte Spain, in which it was found that more and more file sharing sites were moving into the darknet, especially the Tor network. Privacy protection of file sharing users is stated to be successful in this report, as monitoring and take down notices known from the Cleartnet are not working in the Tor network. In combination with cryptocurrencies like Bitcoin, Tor is identified as a significant challenge for anti-piracy efforts.

In the same year a report by Inteliagg (Inteliagg, 2016) concluded that 29% of analyzed Tor hidden services addressed file-sharing information, significantly more than drugs (4%), for example.

A report published in 2018 by irdeto (irdeto, 2018) shows the still high numbers of P2P file sharing. In 2017 6B downloads of TV shows and 4.6B downloads of movies were monitored in the BitTorrent network. Privacy mechanisms are not mentioned in this report.

CONCLUSION

File sharing networks for the illegal distribution of copyrighted material and the darknet were synonyms in the 2000s. Since then, the term darknet has become more connected to privacy networks like Tor. However, the development of monitoring technology to fight online piracy has also changed the file sharing networks. While many users still use file sharing without privacy protection, the amount of file sharing among networks like Tor and I2P has become significant. For Tor, the use of file sharing has even been discouraged officially due to the vast amount of traffic it causes.

Content shared via file sharing darknets seems to be similar to other file sharing networks and consists of movies, TV shows, music, pornography and software. In freenet, the amount of child pornography is said to be alarmingly high. This is a good indicator of the risks of privacy networks: anonymity and the lack of censorship provide tools also attractive for criminal activities far beyond copyright violations.

ACKNOWLEDGMENT

This work was funded by the BMBF project "PANDA". It was made possible by the contributions of our students Karola Marky, Annika Schaefer, Paul Mohr and Philipp Norbert Skrinjar.

REFERENCES

- Aked, S. (2011). An investigation into darknets and the content available via anonymous peer-to-peer file sharing. In *9th Australian information security management conference* (p. 10). Academic Press.
- Alexa. (2016, July). *The top 500 sites on the web*. Retrieved from <http://www.alexa.com/topsites/countries;1/DE>
- Anonym. (n.d.). *Binarynewsgroups*. Retrieved from <http://www.usenetguide.de/Usenet/BinaryGroups.htm>
- Antoniades, D., Markatos, E. P., & Dovrolis, C. (2009). One-click hosting services: a file-sharing hideout. In *Proceedings of the 9th acm sigcomm conference on internet measurement* (pp. 223–234). 10.1145/1644893.1644920
- Astolfi, F., Kroese, J., & van Oorschot, J. (2015). *I2p-the invisible internet project*. Media Technology, Leiden University, Web Technology Report.
- Banerjee, A., Faloutsos, M., & Bhuyan, L. (2007). The p2p war: Someone is monitoring your activities! In *International conference on research in networking* (pp. 1096–1107). Academic Press.
- Bellovin, S. (2001). Security aspects of napster and gnutella. In *2001 USENIX annual technical conference*. USENIX.
- Biddle, P., England, P., Peinado, M., & Willman, B. (2003). The darknet and the future of content protection. In J. Feigenbaum (Ed.), *Digital rights management* (pp. 155–176). Berlin: Springer Berlin Heidelberg. doi:10.1007/978-3-540-44993-5_10
- Biryukov, A., Pustogarov, I., Thill, F., & Weinmann, R.-P. (2014). Content and popularity analysis of tor hidden services. In *2014 IEEE 34th international conference on distributed computing systems workshops (icdcs)* (pp. 188–193). IEEE. 10.1109/ICDCSW.2014.20
- Blond, S. L., Manils, P., Abdelberi, C., K^aafar, M. A., Castelluccia, C., Legout, A., & Dabbous, W. (2011). *One bad apple spoils the bunch: Exploiting P2P applications to trace and profile tor users*. Retrieved from <http://arxiv.org/abs/1103.1518>
- Chaabane, A., Manils, P., & Kaafar, M. A. (2010). Digging into anonymous traffic: A deep analysis of the tor anonymizing network. In *2010 fourth international conference on network and system security* (pp. 167–174). 10.1109/NSS.2010.47
- Chothia, F.-S. T., Chothia, T., & Chatzikokolakis, K. (n.d.). A survey of anonymous peer-to-peer. In *Proceedings of the IFIP international symposium on network-centric ubiquitous systems (ncus 2005)*. Springer.

Chothia, T., Cova, M., Novakovic, C., & Toro, C. G. (2012). The unbearable lightness of monitoring: Direct monitoring in bittorrent. In *International conference on security and privacy in communication systems* (pp. 185–202). Academic Press.

Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. (2001). Freenet: A distributed anonymous information storage and retrieval system. In *Designing privacy enhancing technologies* (pp. 46–66). doi:10.1007/3-540-44702-4_4

Cohen, B. (2003, May). *Incentives build robustness in bittorrent*. Retrieved from <http://bittorrent.org/bittorrentecon.pdf>

D'ecary-H'etu, D., Morselli, C., & Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among warez hackers. *Journal of Research in Crime and Delinquency*, 49(3), 359–382. doi:10.1177/0022427811420876

Deloitte. (2016). *European union intellectual property office report: Research on online business models infringing intellectual property rights*. EUIPO.

Egger, C., Schlumberger, J., Kruegel, C., & Vigna, G. (2013). Practical attacks against the i2p network. In *International workshop on recent advances in intrusion detection* (pp. 432–451). Academic Press.

Goldman, E. (2003). Warez trading and criminal copyright infringement. *J. Copyright Soc'y USA*, 51, 395.

Intelliagg. (2016). *Deeplight: Shining a light on the dark web*. Author.

irdeto. (2018). *The piracy landscape: Has web video replaced peer-to-peer?* Author.

Isdal, T., Piatek, M., Krishnamurthy, A., & Anderson, T. (2011). Privacypreserving p2p data sharing with oneswarm. *Computer Communication Review*, 41(4), 111–122. doi:10.1145/1851275.1851198

Kang, C. (2012). Megaupload shutdown raises new internet-sharing fears. *The Washington Post*.

Kroemer, J., & Sen, E. (2006). *No copy: die welt der digitalen raubkopie* (Vol. 24). Klett-Cotta.

Li, B., Erdin, E., Gunes, M. H., Bebis, G., & Shipley, T. (2013). An overview of anonymity technology usage. *Computer Communications*, 36(12), 1269–1283. doi:10.1016/j.comcom.2013.04.009

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008). Shining light in dark places: Understanding the tor network. In *International symposium on privacy enhancing technologies symposium* (pp. 63–76). 10.1007/978-3-540-70630-4_5

MPAA. (2006). *The pyramid of internet piracy*. Retrieved from [http://www.mpaa.org/pyramid of piracy.pdf](http://www.mpaa.org/pyramid%20of%20piracy.pdf)

Nelson, T. H. (1981). *Literary machines: The report on, and of, project xanadu, concerning word processing, electronic publishing, hypertext, thinkertoys, tomorrow's intellectual revolution, and certain other topics including knowledge, education and freedom*. Academic Press.

Piatek, M., Kohno, T., & Krishnamurthy, A. (2008). Challenges and directions for monitoring p2p file sharing networks - or - why my printer received a dmca takedown notice. Hotsec.

Pouwelse, J., Garbacki, P., Epema, D., & Sips, H. (2005). The bittorrent p2p file-sharing system: Measurements and analysis. In *International workshop on peer-to-peer systems* (pp. 205–216). Academic Press.

- Prusty, S., Levine, B. N., & Liberatore, M. (2011). Forensic investigation of the oneswarm anonymous filesharing system. In *Proceedings of the 18th acm conference on computer and communications security* (pp. 201–214). 10.1145/2046707.2046731
- Saroiu, S., Gummadi, K. P., & Gribble, S. D. (2003). Measuring and analyzing the characteristics of napster and gnutella hosts. *Multimedia Systems*, 9(2), 170–184. doi:10.1007/00530-003-0088-1
- Schimmer, L. (2009). Peer profiling and selection in the i2p anonymous network. Petcon 2009.1.
- Smith, S. (2003). From napster to kazaa: The battle over peer-to-peer filesharing goes international. *Duke law & Technology Review*, 2(1), 1–9.
- Syverson, P., Dingledine, R., & Mathewson, N. (2004). Tor: The secondgeneration onion router. Usenix Security.
- Wood, J. A. (2009). The darknet: A digital copyright revolution. *Rich. JL & Tech.*, 16, 1.
- Yang, J., Ma, H., Song, W., Cui, J., & Zhou, C. (2006). Crawling the edonkey network. In *2006 fifth international conference on grid and cooperative computing workshops* (pp. 133–136). 10.1109/GCCW.2006.29
- Zhang, C., Dhungel, P., Wu, D., Liu, Z., & Ross, K. W. (2010, March). Bittorrent darknets. In *2010 proceedings IEEE infocom* (pp. 1–9). IEEE. doi:10.1109/INFCOM.2010.546196

ADDITIONAL READING

- Biddle, P., England, P., Peinado, M., & Willman, B. (2003). The darknet and the future of content protection. In J. Feigenbaum (Ed.), *Digital rights management* (pp. 155–176). Berlin: Springer Berlin Heidelberg. doi:10.1007/978-3-540-44993-5_10
- Lasica, J. D. (2005). *Darknet: Hollywood's war against the digital generation*. Hoboken, NJ: Wiley.
- Röttgers, J. (2003). Mix, burn & RIP: das Ende der Musikindustrie.
- Wood, J. A. (2009). The darknet: A digital copyright revolution. *Rich. JL & Tech.*, 16, 1.

KEY TERMS AND DEFINITIONS

Darknet: From the perspective of copyright violations, any network used for the illegal distribution of files can be called a darknet. From a privacy perspective, a darknet is a network providing anonymity for its participants.

File-Sharing: Offering and transferring digital files via various channels of the internet, usually in a decentralized manner.

IP Address: Internet protocol address, usually the basic identifier of a computer participating in the internet. It can be seen as a pseudonym of the user of the computer and can be connected to the identity of the user by his internet service provider.

Peer-to-Peer Network: A network of nodes with usually equal rights and responsibilities. The nodes are usually computers of Internet users where a software with the peer-to-peer protocol is running.

Tor: Short for The Onion Router. A privacy network based on onion routing and encryption.

Warez: Term for illegal digital goods, usually software or multimedia files.

Academic Integrity of Global Digital Masked Bandits Lurking the Deep and Dark Web

David B. Ross

Nova Southeastern University, USA

Julie A. Exposito

Nova Southeastern University, USA

Melissa T. Sasso

 <https://orcid.org/0000-0001-6578-8239>

Nova Southeastern University, USA

Cortney E. Matteson

Orange County School District, USA

Rande W. Matteson

Nova Southeastern University, USA

INTRODUCTION

Educators in the K-20 system are faced with an important issue as it pertains to academic writing and research. There are many studies on academic dishonesty and cheating at all levels of education. Administrators and faculty in education need to be aware of the entrepreneurial gravity of this scheme and be proactive in communication by informing all stakeholders to develop policies to this academic epidemic. This article will also research the motives of academic dishonesty, deep web schemes to defraud, avoidance of criminal prosecution, and non-conventional intellectual warfare while making recommendations for internal change and reform. The purpose of this article is to enlighten practitioners and researchers to include students and educational administrators about the growing concern of plagiarism, unintentional plagiarism, defrauding funding sources, governmental agencies, educational institutions, perspective employers, and affixing serious long-term consequences and liability to participants and placing a negative stigma on brand reputation and further stress on academia.

BACKGROUND

There is a chasm between policy and research, and there is a need to increase the policy impact of educational research (Gillies, 2014). Gillies (2014) claimed knowledge activism is one method that research can influence policymaking. Fowler (2013) commented that in the event of a public problem, policymakers must have a policy process to examine any policy issue that is under debate. Public policy should be grounded by research, especially research on the phenomenon of academic integrity in a

DOI: 10.4018/978-1-5225-9715-5.ch012

technologically driven society, especially with access to the deep web. When faculty at institutions of higher education recognize students' academic dishonesty tactics, they must *take corrective action* by following the university's policies by guarding the integrity of the course curricula (Larkin, Szabo, & Mintu-Wimsatt, 2017). Löfström, Trotman, Furnari, and Shephard (2015) compared academic integrity to a skill. Academic dishonesty is a phenomenon witnessed in higher education where the decision to cheat is a deliberate choice for students (Seals, Hammons, & Mamiseishvili, 2014). Moten, Fitterer, Brazier, Leonard, and Brown (2013) explicated that due to the lack of face-to-face interaction between students and faculty and because of online learning, students have a stronger opportunity to engage in cheating, which is described as defrauding the intellectual property of the institution, plagiarizing, and violating university/college policies.

No part of the educational system is immune from dishonest and illicit non-traditional schemes to attack its integrity. Although this behavior is prevalent in higher education, it is also a disturbing phenomenon witnessed at all educational levels in society. McCabe, Treviño, and Butterfield (2001) made mention of a study that by the time high school students enter college, they have had previous years of practice regarding academic dishonesty. In addition, if college freshman continues to cheat their next few years while in college, they consider high school to align with college practices of academic dishonesty. McCabe et al. conducted a ten-year research study of college students regarding cheating that occurs in academic institutions to include the importance of having integrity/honor code policies in place. Research indicates that due to the personal and professional challenges students face today, they tend to practice dishonest study habits, therefore the reason for the implementation of policies and honor codes (McCabe, Treviño, & Butterfield, 2001). McCabe et al. explained that

No campus can assume that its students, incoming or returning, will take the time to familiarize themselves with campus rules about academic integrity on their own. Even if they did, an institution's failure to emphasize for its students the high value it places on academic integrity sends the message that it is not a high priority. (p. 231)

Understanding the reasons, although not condonable, for cheating is an important component in policy decisions (Marsh, 2011). Preserving academic integrity is a topic for all stakeholders that have been challenged by the onset of new technology and changed viewpoints of the millennial generation (Dyer, 2010; Moten, Fitterer, Brazier, Leonard, & Brown, 2013; Trenholm, 2007). The increase of technology usage has increased violations of academic integrity: an increased connectivity, collaboration, and social networking (Dyer, 2010; Jiang, Emmerton, & McKauge, 2013; Marsh, 2011). Online courses mean reduced supervision and greater availability for collaboration. Another challenge for educators includes teaching students correct ways to use and cite online sources. A digital divide exists between instructors and students. *Millennials* are adept at using computers, smartphones, and new technologies to gain answers for assignments, exams, or papers (Dyer, 2010).

A notable study undertaken by the Josephson Institute on Ethics of nearly 30,000 public and private high school students in the Los Angeles California area found 30% admitted to stealing from retail stores and 25% admitted to stealing from friends and family members (Zicari, 2008). Zicari (2008) noted another 64% admitted to cheating in school examinations, and 38% admitted to cheating multiple times in their school assignments. Thirty-six percent of students admitted to stealing digitized academic work by plagiarism tactics from the Internet. The students who participated in the study stated 93% believed their behavior was ethical. Seventy-seven percent of the student participants stated they are far more ethical than their peers. This is an epidemic in today's educational system to include the entire world.

The deranged Unabomber, Theodore Kaczynski, wrote in his manifesto how the world would be far more dangerous and destructive with conflicts among people, processes, and digital technology. Social acceptance of apathy and corrupt practices does not provide for a healthy society of critical thinkers with the skills to advance communities, people, and nations. This technology is causing our usurping of critical thinking by taking the easy way out, which is one reason why students cheat. Diamond (2017) quoted Andrew Sodroski, a television executive producer, regarding Kaczynski's manifesto as, "What the manifesto has to say about our relationship with technology and with society is truer right now than it was when Ted published it" (para. 5). After all these years, Kaczynski was correct, as the Internet has brought people closer to information, but also false information and illegal means to obtain information. Students and other researchers have become dependent upon the technology and have lost reason by allowing technology to take over their critical thinking to merely plagiarizing and searching for ghostwriters than researching and writing their papers, articles, and other published work.

Once a service, such as technology, has been made available, people could decide, why not use it, is at all that bad or illegal? Like any crime, people feel that if it is wrong and no one is stopping them; why not continue to use the information online? In addition, people feel that if it is online, it must be true. Kaczynski (1995) wrote about how people can be dependent on the technology as well as the mass-communication media.

In many cases the new technology changes society in such a way that people eventually find themselves forced to use it. . . . Another reason why technology is such a powerful social force is that, within the context of a given society, technological progress marches in only one direction; it can never be reversed. Once a technical innovation has been introduced, people usually become dependent on it, unless it is replaced by some still more advanced innovation. (p. 16)

Creative cheating schemes have become commonplace. The quick and easy approach to academic studies has eroded the quality, rigor, and derailed students' critical thinking skills of students throughout the world. Subscribers and payees of paper mills and the compliment of ghostwriters all collectively provide *Material Support* to international crime cartels, a federal felony 18 USC 2339A. It is reasonable to have conversations that global digital sycophants who have used clever schemes to defraud, cheat, have attacked authentic leadership and game our critical American infrastructures with agendas that we argue are misaligned to our cultural norms, our educational system, and our Democratic foundation. Additionally, the construct of academic integrity and consequences of academic dishonesty is a challenge that academic institutions face as the international population increases at American universities and colleges (Gillespie, 2012).

FOCUS OF THE ARTICLE

Blum (2009) admonished there must be communication about plagiarism between students and faculty, and international students must be cognizant of institutional policy on academic integrity. Cohen (2007) illustrated that variances in cultural could be misinterpreted with negative consequences for international students. Furthermore, it was discovered that ideas of cheating and students' shared work, which is acceptable in numerous cultures. Surprisingly, this is viewed as an honorable act in having the ability to aid others in this manner, as sharing of information does not constitute any behaviors of honesty, character, and integrity (Cohen, 2007). Students do not consider that academic dishonesty is unethical,

and in some cultures, it is considered inclined, a challenge and/or acceptable behavior if noticed by their faculty. Numerous cases have demonstrated that students were insulted by allegations of wrongdoing, and due to their moral beliefs, believe it would be seen as a lack of character by not assisting their peers. Cohen discussed an event that pertained to a student from Asia who took great joy in the ability to cheat; however, without hesitation would admit to the student's unethical behavior if caught. Another situation deemed acceptable is the forgery of documents to leave native countries. If for the greater good, it is not perceived to be an act of dishonesty. Integrity in higher education is a culturally derived term and has various meanings to individuals from a myriad of cultures. International students contribute to American institutions of higher education; therefore, the policymakers within higher education are responsible for minimizing academic integrity cultural barriers (Smithee, 2009).

Academic misconduct. Weber-Wulff (2014) identified various forms of academic misconduct: (a) contract cheating, (b) falsifying data, (c) ghostwriting, (d) honorary authorship, (e) paper mills, (f) plagiarism, and (g) unknown ghostwriters. Academic cheating, as noted by several researchers, have concluded that within schools and universities of many countries, forms of dishonesty is not a novel occurrence. It has been observed that students like to utilize a plethora of methods to obtain what one would consider undeserved privileges that comprise of masking the truth in their research (Bachore, 2016; Iberahima, Husseinb, Samatc, Noordind, & Daude, 2013; Sarita, 2015).

Contract Cheating

Contract cheating is the process of bidding between independent contractors for assignments that have been uploaded to a website. The client selects an author based on the lowest bidding price, and services are paid through PayPal (Weber-Wulff, 2014).

Walker and Townly (2012) found there is an increase in contract cheating, and Wallace and Newton (2014) investigated postings from the freelancer and TransTutors website to postulate whether a shorter time frame for the completion of assignments would decrease the incidences of contract cheating. Contract cheating evades plagiarism detection software since the submitted work is original work.

Falsifying Data

Falsifying data is the manipulation of data to meet personal agendas in biased research. In a qualitative study, researchers have to write sections on ethical considerations, trustworthiness, and potential research bias. The ethical considerations are based on how the researcher maintains the ethics of the study and preserves anonymity and confidentiality while keeping documents and digital recordings secure. Trustworthiness demonstrates that the study is valid and reliable. Inaccuracy and a lack of corroborating evidence affect research leading to misinterpretation of research and falsification of data. The researcher must account for potential bias and remain subjective and neutral to various viewpoints (Creswell, 2013).

Ghostwriting

Ghostwriting is the process where an author does not receive acknowledgment for writing assignments. Companies hire ghostwriters to write custom-written papers. Because the company acts as an intermediary, the ghostwriter remains anonymous. There is no contact between the client and the ghostwriter (Weber-Wulff, 2014).

Paper Mills

A paper mill maintains papers collected with an author's permission in a large database. The customer purchases access to this database under the pretense of learning to structure the paper. The paper mill cautions the client to use the paper only as a resource. As cited in Wallace and Newton (2014), Turnitin found 7% of higher education students have reported purchasing a paper during their undergraduate studies.

Plagiarism

Based on literature discovered, researchers have classified many types of plagiarism: (a) copy and paste, (b) translations, (c) disguised plagiarism, (d) shake and paste collections, (e) clause quilts, (f) structural plagiarism, (g) pawn sacrifice, (h) cut and slide, (i) self-plagiarism, and (f) other dimensions like collusion. There has been a hike in plagiarism over the past decade due to the access to technology. Plagiarism is described as including other researchers' thoughts, verbiage, data and/or findings (Bachore, 2016; Sarita, 2015; Weber-Wulff, 2014).

Unknown Ghostwriters

Weber-Wulff (2014) described an "unwitting ghostwriter" to be a thesis writer with archived work on a compact disk with a digital version at the university library. Students access these digital versions to modify, use, and claim ownership to the thesis. Technology has revolutionized higher education and has provided a vast amount of information accessible to students. The significant number of companies advertising editing services indicate a widespread problem of academic misconduct (Weber-Wulff, 2014). However, are students seeking editors for format only, or rather editors to create and/or rewrite existing papers? Institutions use plagiarism detection software to compare essays against a database of work, but many paper mill companies guarantee original work by a ghostwriter and screen the work for plagiarism before distributing it to clients. The cost ranges from \$20.00 to \$40.00 depending on the subject and turnaround time needed. Software like Turnitin is used to find counterfeit papers but does not intercept custom papers. Wallace and Newton (2014) believed contract cheating to be a problem; although this phenomenon is widespread, there are few studies and few approaches addressing it. Theoretically, contract cheating is original work that avoids detection from originality detection software. This makes it difficult to estimate the extent of contract cheating. Wallace and Newton suggested a reduction in turnaround time for due dates of assignments may give students less time to contract an independent contracted writer, but would not eliminate the occurrence of contract cheating. Most likely, the student will have a due date, but if a ghostwriter does not fulfill his or her obligation to the student, the ghostwriter is also committing fraud by receiving funds and not adhering to the contract for the student.

Fraud

Academic dishonesty is a concern for institutions of higher education as the increase in technology provides a path to new ways of committing academic fraud and electronic dishonesty (Wallace & Newton, 2014). Stanford University issued an alert of a high number of students suspected of cheating. Even though students accept the terms of the honor code, students are risking the consequences of cheating (e.g., failing grade, suspension, expulsion). In 2013, 83 students violated the honor code; a first violation results in a suspension of one term and 40 hours of community service (Mercury News, 2015).

The conduct of cheating violates both federal and state felony statutes-law(s), and a person(s) or institution can be criminally charged-convicted individually or in a conspiracy case. Double jeopardy does not imply if charged or convicted in both the federal and state courts based on the same conduct in the defense argument, but for the purpose of this paper, the focus will only be based upon the federal law (i.e., U.S. Criminal Code). Aside from the criminal liability outlined, there are real concerns for civil suits, which can also be applied simultaneously for the same conduct as the criminal charges. The Federal False Claims Act is a tool that can reign in unethical conduct and encourages the reporting of unethical conduct and violations of federal law. Many states have adopted the provisions of the Federal False Claims Act; any person or institution can be dually charged with violations of federal-state False Claims Act offenses arising from the same conduct.

By applying the law to cheating scandals, it sends a clear message to stakeholders to discourage individuals from cheating. Trying to assert a defense of ignorance fails to provide legal protection if the person or institution knows or suspects fraud or organized schemes to cheat or defraud. For example, any person or institution having personal knowledge of any conduct that is outlined in this paper and other activities defined by statute as illegal conduct can lead to the felony prosecution of persons and or institutions that fail (Misprision of a felony) to report any conduct which is illegal (18 USC § 4).

Under the federal criminal code, it is important to underscore the law of conspiracy (18 USC § 371 & 1349). In summary, this provision of the law includes any (overt acts) or attempt(s) to do an act in violation of a crime; the crime is punishable under the same provisions as if the act had been completed. Under the theory of a conspiracy, any person-business in the conspiracy is liable for the acts of others whether they know the others involved and the statements of others are attributable to others. The 18 USC 1346 is a federal criminal statute that covers Honest Services for any conduct that leads to an artifice or scheme to defraud.

Any proceeds or property acquired by means of academic cheating are subject to either federal or state administrative-criminal asset forfeiture proceeding. Thus, there is an added disincentive for engaging in the conduct presented in this paper (18 USC § 1956). It is nearly impossible to effectively escape criminal-asset forfeiture liability in these examples. The suggestion is to remain proactive and develop affirmative programs and policies aimed at preventing and eradicating serious forms of educational cheating.

At the University of California, San Diego, 600 students cheated in 2014 by copying tests, using notes, helping others, or purchasing papers online. As a response, the university implemented an Academic Integrity Office to handle student cheaters (Regents of the University of California, 2015). Students who earn grades through academic dishonesty undermine values of the institution; serious consequences include the destruction of academic records and reputation and an inability to matriculate (Dyer, 2010).

CNN reported cheating on papers is a “booming Web business” and reported 90% of the requests for online academic papers to come from the United States. DomainTools purported essaywriters.net solicits writers to write these papers research papers, book reports, and coursework on syllabi. Various paper mill enterprises make claims they offer original writing services provided to customers as a reference only and are not to be used without proper citations. This assertion is deceptive and does not offer any statement reporting the true identity of the ghostwriters who authored the work. Clearly, there are few real customers other than students who purchase academic papers to defraud professors, academic institutions, financial loan service providers, and administrative-regulatory oversight agencies. It is not possible to sell the volume (based upon customer testimonials who admit to using the paper mill services to order, purchase, and submit papers to schools and colleges to pass courses) of scholarly papers for non-academic use.

There is a myriad of clever schemes designed by paper mill enterprises that actively solicit customers and students. These digital masked bandits conspire and consequently defraud academic institutions/loan servicing providers, and federal-state administrative and regulatory oversight agencies by using these fraudulent schemes with the intent to misrepresent.

An example of a simple scheme includes federal felony crimes of mail or wire fraud communications technology and other means to communicate the scheme including regular or express mail services. In summary, paper mills must operate using means to communicate. Under the federal mail and wire act, any person-business or other entity involved in a scheme to defraud (attempts are included) using the mail or wire systems are crimes (18 USC § 1341 and 1343).

A federal fraud conviction is most likely to include mandatory prison time, fines, or probation. If sentenced to prison, the sentence could range from 6 months to 30 years for each act. Home confinement is an alternative sentence that is rarely applied. The offender is now labeled a convicted felon restricting the rest of his or her life. Fines are another punishment for a violation of fraud and could be as much as a \$250,000 fine for each violation. Finally, restitution and probation are additional sentences imposed with a guilty conviction of fraud (Theoharis, 2015).

The volume of activity and sales of papers is unquantified but remains staggering if one were to believe the published testimonials on the websites of paper mills and YouTube posts endorsed by student customers. It is likely the paper mill services under report and or fail to report earnings to federal and state taxing authorities which also become crimes (26 USC § 7201).

A national investigative-enforcement strategy could prevent-control this problem. Adding enhanced crimes, such as false statements or causing/keeping false records: (a) student grades and educational reports (18 USC § 1001), (b) theft (18 USC § 666), (c) the Racketeer Influenced and Corrupt Organizations (RICO) Act (18 USC § 1961-1968) and (d) financial institution fraud crimes (18 USC § 1344), Honest Services Fraud 18 USC 1346 and 1349 (Attempts) can be applied as countermeasures and investigative tools. Each carries additional criminal sentences and asset forfeiture penalties (18 USC § 1956).

Motives for Academic Dishonesty

It is essential to bring up cheating as early as possible, as it will aid in guaranteeing ethical behavior in practice since academic dishonesty is linked with unethical business practices (DiVall & Schlesselman, 2016; Iberahim, Hussein, Samat, Noordin, & Daud, 2013). As educators, it is difficult to comprehend why students continue to cheat and or plagiarize, however, as educators, we have also forgotten the extreme pressures that students experience. Now, this in no way, shape or form means that educators must water down the curriculum to prevent cheating, but it gives insight as to one of the possible reasons why it occurs. More specifically, DiVall and Schlessman (2016) indicated that pressure, from students, is heightened by the students' peers or even families. It was further illustrated that having such pressure can cause students to be greatly grade-oriented, instead of being outcome-oriented.

According to research, the students desire to get ahead is one of many reasons to engage in academic misconduct. Other reasons for plagiarizing and cheating are due to, being scared of failing, having bad time management skills, and the longing to help a school colleague (DiVall & Schlessman, 2016). Naghdipour and Emeagwali (2013) further indicated alternate reasons for academic misconduct, which comprise of both psychological and individual factors such as, "gender, low GPA, age, narcissism, competitive achievement and contextual factors such as the existence of honor codes, disciplinary rules and learning environment" (p. 261). Iberahim et al. (2013) explicated that research illustrated an abundance

of reasons that students engage in academic misconduct: (a) grades, (b) big classes, (c) struggle for jobs, (d) cheating culture that is common within the community, (e) sincere deficiency of comprehending of what is plagiarism, (f) personal values, (g) no respect for authority, (h) opportunity, and (i) cheating having a nominal effect on others.

Results for a study conducted by Iberahim et al. (2013) revealed that a majority of students took part in academic dishonesty, as the faculty member was okay with that form of behavior. DiVall and Schlessman (2016) stated that faculty members could lower the percentage of students cheating by fabricating seating charts or issuing various versions of tests on test day. However, faculty members have indicated that taking these measures have proved to be time-consuming, and therefore, did not implement these procedures. Moreover, as technology continues to progress, it has deemed to assist students in cheating more and make it further challenging for professors to prevent this misconduct (DiVall & Schlessman, 2016; Naghdipour & Emeagwali, 2013). University administrators need to make strict policies and procedures as well as streamline the process to hold students, faculty, and other stakeholders accountable.

Academic integrity threatens ethical leadership and citizenship and permeates all aspects of life (a) validity of assessments, (b) equity in grading, (c) diminishes the reputation of institutions of higher education, (d) workplace behavior, and (e) societal context. Academic dishonesty has social consequences reaching far beyond the classroom (Dix, Emery, & Le, 2014). There is a relationship between human values and ethical leadership. Moral education is the center of virtue ethics (Marsh, 2011). Marsh (2011) conducted a mixed-mode analysis to find circumstances to justify cheating. Marsh surveyed 401 undergraduate students at a Carnegie I research university, 66% were freshman (59% were female, 41% male), and 7% spoke English as a second language. One hundred and forty-four students claimed there are circumstances that justify cheating. There were six reasons that justified cheating: (a) denial of responsibility, (b) denial of injury, (c) condemning the condemners, (d) self-fulfillment, (e) appeal to higher loyalties, and (f) denial of the victim. There were subcategories (a) accidents, (b) crisis, (c) scapegoating, and (d) accidental plagiarism. Additional reasons included material or tests that were too difficult or lack of explanation of the material. Students reported paraphrasing might be considered plagiarism.

Other driving forces for academic misconduct include individual pressures, time constraints, and availability of online sources (Jiang, Emmerton, & McKaige, 2013). Blum (2009) contended competency-based education, increased the cost of college tuition, and the value of earning power contribute to the culture of academic dishonesty in higher education. Shifting generational attitudes and information technology are two factors that perpetuate the lack of academic integrity (Dyer, 2010; Manly, Leonard, & Riemenschneider, 2014). In fact, Manly, Leonard, and Riemenschneider (2014) claimed an instructor-student disparity existed over the perception of cheating. Instructors held a different viewpoint of cheating behaviors than students. In most cases, students did not consider behaviors associated with information technology to be cheating, and the top three behaviors using information technology included (a) electronic devices during exams, (b) using ideas from an online purchased paper, and (c) cutting and pasting data from the Internet. Dyer (2010) maintained millennials had worked collaboratively using the Internet since elementary school, and students are not aware that copying and pasting from online resources is a violation of academic integrity. The concept of integrity has evolved, and there is a marked difference in the perception of acceptable academic behavior.

For 10 years, no one knew Dave Tomar, a once ghostwriter who wrote over 3,500 papers, who stated that he engaged in ghostwriting for a living to aid him financially. He started writing papers for students, on all subjects, out of college and worked for other online companies. He initially made 10 to 20 dollars a page and was then paid up to 40 dollars to help students cheat, as he described them as being too lazy

or incompetent. Tomar revealed that in regards to those who are guilty of cheating, it is not an ethical question that one would ask, but rather it is a practical question. Tomar learned of two suspicions while ghostwriting, of which one was that numerous students are given and accept the message that they are going to school to obtain grades as well as a degree. His second suspicion was the number of students who are going to school without adequate preparation and how students are deficient in critical skills.

As early as 2003, the Secretary-General for Interpol Ronald Noble testified before the House Committee on International Relations in the United States Senate and stated the link between the trafficking of Intellectual Property Crime Piracy, or theft of trade patents and business competitiveness-sabotage has direct ties to funding global Terrorist groups including Al Qaeda, Hezbollah, and Hamas. Various other experts cited in the review, have noted the vast wealth attributed to these crimes requires the use of capitalistic systems to be successful. Digital masked bandits can lurk in the dark web stealing trillions of dollars and remain relatively anonymous and hard to detect by traditional investigative means (Williams, 2008).

Ghostwriting Process

A student has a limited time to complete a paper, and a quick online search of *paper mills plagiarism mills* or *essay mills* produces several results. Although many of these companies claim to help the professional, the services are geared toward a specific client: the student. The websites offering academic papers boast an endless amount of testimonials; this information can be used against the company's interest and can be used as evidence in fraud cases. There are YouTube tutorials students have explained how to use paper mills. To illustrate the popular stance on academic dishonesty, one student explained successful strategies for cheating on an exam; this post received 20,947 likes and 6,560 dislikes (Ferasweelz, 2012). This evidence can be used in both state and federal cases and could establish a RICO investigation by the federal system; additionally, laws vary within each state (VOA Special English, 2014).

According to admitted scholarship ghostwriter Tomar (2012), this problem is rampant. As an illustration, a student receives an assignment with the professor's criteria, expectations, rubric, scoring guide, and format rules. The potential client searches for a paper mill company and selects one based on various factors. The paper mills have ghostwriters who could be scholars such as professors, graduate students, and/or freelance writers. Papers are written for all academic levels and disciplines and are not triggered by Turnitin or any other program that will detect plagiarism. The client includes payment information and then posts the topic on the paper mill board, which is comparable to a bulletin board format. A ghostwriter contacts the client directly to discuss the specifics of the paper based on the guidelines. The client's credit card is charged, and then the contracted writer begins working on the paper. By entering into an agreement, both parties agree to accept the resulting obligations and consequences. The ghostwriter then sends a final copy via email. The client can review the document and discuss possible changes or edits. If there are changes that will be made, there will be further discussion about pricing. The student only has to write his or her name on the title page of the paper and submit it to the professor, usually by email. This paper will not trigger Turnitin as plagiarized work, so then the professor grades it. At this point, the student has now stolen a grade, which is something of value.

Consider the hundreds of thousands of grades that are stolen and reported to various oversight agencies causing them to keep and transmit fraudulent data and to fund the student's education in this scheme to defraud. This conduct can be defined as theft and fraud because something of value (e.g., academic grade) was stolen. The testimonials posted on paper mill websites and YouTube indicates that income

could exceed hundreds of billions of dollars in revenue from these services. Tomar (2012) reported the conduct is unregulated and out of control. These examples underscore what is defined in the above sections as additional-potential crimes which include (a) false statements, (b) wire fraud, (c) mail fraud, (d) conspiracy, (e) RICO, (f) money laundering, and (g) financial institution fraud (e.g., banks, PELL, VA, financial aid), and (h) theft.

Consequences. Now that the student is involved in the overall scheme or a conspiracy, everyone involved in the paper mill companies (e.g., owners, ghostwriters, institutions, students) committed numerous violations of law and may be involved in an ongoing conspiracy. The vendor, end user, employers, governmental and private sector funding, and regulatory authorities and sources along with K-20 administrators and the faculty involved are all co-conspirators in a clever criminal scheme to defraud a myriad of entities.

Phony grades from students using fraudulent scholarly work from paper mills are ultimately reported, maintained, and transmitted to federal and state departments of education (and related administrative and regulatory agencies). This represents false record-keeping, and there exists no accrediting agency that has the means to track this information (18 USC § 1001).

As a result of this illegal conduct by paper mills, considerable amounts of revenue may be produced and laundered. The assets/monies are subject to asset seizure and forfeiture; this is an added incentive for law enforcement to initiate a criminal investigation into these organized schemes to defraud (18 USC § 1001).

Investigation

Academic fraud needs to be approached much like any other fraud case. In order to curtail academic dishonesty, proactive initiatives are generally productive options. Investigators should develop cooperating witnesses-sources, collect testimonials and other promotional evidence found on paper mill websites and YouTube. Investigators should follow the flow of money through electronic wire intercepts, tax returns, credit cards, and bank accounts, as well as subpoena records and financial-records search warrants. In the investigation, the Internet service provider (ISP) will provide a narrative content with the final goal of tracking the crimes all conspirators: students, witnesses, ghostwriters, and companies.

Additional Players

If an institution or individual has knowledge of a crime (schemes to defraud) and fails to report it, it is a violation of the US Code 18 Section 4 (Misprision of a felony), which is a federal felony violation of a law. In the recent cases of systemic academic corruption, the Atlanta Public School administration and faculty engaged in an ongoing scheme to defraud various organizations and its chieftains-participants landed lengthy prison sentences.

SOLUTIONS AND RECOMMENDATIONS

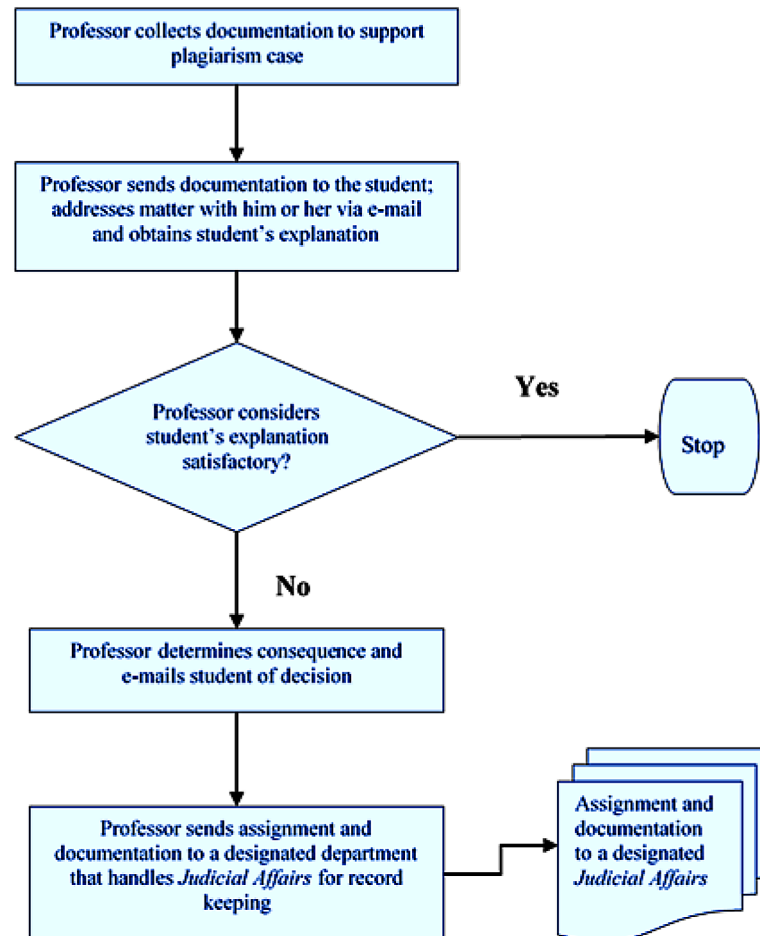
Weber-Wulff (2014) admonished the question of intent: (a) unintentional, (b) honest mistake, (c) poor referencing, or (d) purposeful deception may be difficult to discern, but university and college policy-makers need to address the problem of academic misconduct. Strategies to reduce plagiarism will affect learning, cheating, campus culture, and institutional image (Dix, Emery, & Le, 2014). Using online

detection services, providing plagiarism workshops, and educating students and faculty of the consequences of academic dishonesty may decrease the number of occurrences. Plagiarism policies need to be developed by training students and faculty, establishing a transparent policy, and testing random dissertations, theses, and papers (Weber-Wulff, 2014). By turning in early versions of term papers, research papers, and essays, students will be encouraged to complete original work.

Professors, teachers, and other personnel who detect plagiarism-unintentional plagiarism while grading papers need to have teachable moments for students who may not be aware of this type of behavior. Policy makers in universities and colleges, including the K-12 system, should have a policy in place that not only detects possible plagiarism but how to collect the documentation to support the detection. In addition, this policy should illustrate the process to determine whether a student was in violation of the plagiarism-unintentional plagiarism directives and if so create a paper trail and flowchart as described in Figure 1.

Löfström et al. (2014) explored the definition of academic integrity, how it should be taught, and whose responsibility it is. All surveyed groups agreed on several components of academic integrity including but not limited to (a) the importance of the research process, (b) knowledge of faculty to teach academic integrity, (c) academic integrity is more than following rules, and (d) ignoring minor inci-

Figure 1. Protocol for handling plagiarism



dences will not protect the university's reputation. It is essential to know the rules, teach the rules, and follow departmental and institutional processes. The use of honor codes could also be part of the solution (Manly, Leonard, & Riemenschneider, 2014). Gillespie (2012) ascertained academic advisors play a primary role by informing new students about plagiarism, explaining its consequences, and referring new students to campus resources. These academic advisors and faculty should also inform students of *unintentional plagiarism*. Unintentional plagiarism is when students and researchers poorly paraphrase by changing minimal words, changing intended meaning, or using words not part of his or her vocabulary. Additionally, quoting or citing poorly also is considered unintentional plagiarism. Academic integrity can be maintained by (a) educating students, (b) incorporating new technologies and styles of teaching like smartphones and online authorized study groups, and (c) policing students and enforcing policies (Dyer, 2010). Since culture plays a role, advisors should explore the perceptions of academic integrity, faculty from other countries, and other international students (Smithee, 2009).

CONCLUSION

The public policy of plagiarism, editing services, contract cheating, and use of ghostwriting need to be implemented. These policies and issues apply to the university and its business principles. As noted in Table 1, not all universities/colleges have a policy on unintentional plagiarism, nor did they have policies on fraud. This is a phenomenon that must be addressed internally as well as with accrediting agencies. The Center for Academic Integrity (1999) developed seven recommendations for every institution of higher education:

1. Have clear statements, policies, and procedures that are implemented.
2. Inform and educate the community about academic integrity.
3. Practice these procedures from the top down. Follow and uphold them.
4. Have an equitable system to adjudicate violations.
5. Develop programs to promote integrity.
6. Watch trends in technology that affects campus integrity.
7. Assess the efficacy of policies and improve upon existing ones.

Policy needs to be formulated and followed by engagement and commitment. Such initiatives will reduce fraudulent acts. This is so prolific; transnational organized crime syndicates will exploit opportunities to cheat and corrupt our educational system worldwide. Once it has been corrupted and dismantled from a global perspective, society will fail to exist.

REFERENCES

Altbach, P. G., Gumport, P. J., & Berdahl, R. O. (Eds.). (2011). *American higher education in the twenty-first century* (3rd ed.). Baltimore, MD: The Johns Hopkins University Press.

Attempt to evade or defeat tax 26 U.S.C. § 7201

Bachore, M. M. (2016). The nature, causes and practices of academic dishonesty/cheating in higher education: The case of Hawassa University. *Journal of Education and Practice*, 7(19), 14–20.

Bank fraud 18 U.S.C. § 1344

Blum, S. D. (2009, February 20). Academic integrity and student plagiarism: A question of education, not ethics. *The Chronicle of Higher Education*, 55(24), A35.

Cohen, M. C. (2007). *Responding to the barriers to academic success for local international students as an avenue to student success and to the internationalization of a community college* (Order No. 3252965). Available from ProQuest Dissertations & Theses Global. (304734360). Retrieved from <http://search.proquest.com.ezproxylocal.library.nova.edu/docview/304734360?accountid=6579>

Conspiracy to Commit Offense or to defraud United States 18 U.S.C. § 371

Council on Foreign Relations. (2012). *U.S. Education Reform and National Security*. Council on Foreign Relations Press. Retrieved from <https://www.cfr.org/report/us-education-reform-and-national-security>

Diamond, J. (2017). *Flashback: Unabomber publishes his 'Manifesto'*. Retrieved from <https://www.rollingstone.com/culture/culture-news/flashback-unabomber-publishes-his-manifesto-125449/>

Dix, E. L., Emery, L. F., & Le, B. (2014). Committed to the honor code: An investment model analysis of academic integrity. *Social Psychology of Education*, 17(1), 179–196. doi:10.1007/11218-013-9246-2

Dyer, K. (2010). Challenges of maintaining academic integrity in an age of collaboration, sharing, and social networking. In *Proceedings of TCC 2010* (pp. 168-195). Academic Press.

False Statements Accountability Act of 1996 18 U.S.C. § 1001

Ferasweelz. (2012, January 21). *How to cheat on an exam/test (it really works!)* [Video file]. Retrieved from <https://www.youtube.com/watch?v=g1I-7mHKitI>

Fowler, F. C. (2013). *Policy studies for educational leaders: An introduction*. Boston, MA: Pearson.

Fraud by wire, radio, or television 18 U.S.C. § 1343

Gillespie, G. (2012). Guide to advising students about academic integrity. *The Mentor: An Academic Advising Journal*. Retrieved from <https://dus.psu.edu/mentor/2012/03/guide-to-advising-international-students-about-academic-integrity/>

Gillies, D. (2014). Knowledge activism: Bridging the Research/Policy divide. *Critical Studies in Education*, 55(3), 272–288. doi:10.1080/17508487.2014.919942

Iberahima, H., Husseinb, N., Samatc, N., Noordind, F., & Daude, N. (2013). Academic dishonesty: Why business students participate in these practices? *Social and Behavioral Sciences*, 90, 152–156.

Jiang, H., Emmerton, L., & McKauge, L. (2013). Academic integrity and plagiarism: A review of the influences and risk situations for health students. *Higher Education Research & Development*, 32(3), 369–380. doi:10.1080/07294360.2012.687362

Kaczynski, T. (1995). *Industrial society and its future*. Retrieved from <http://editions-hache.com/essais/pdf/kaczynski2.pdf>

Larkin, C., Szabo, S., & Mintu-Wimsatt, A. (2017). Academic integrity of graduate online students in a curriculum and instruction program. *International Research in Higher Education*, 2(4), 1–8. doi:10.5430/irhe.v2n4p1

Laundering of monetary instruments 18 U.S.C. § 1956

Löfström, E., Trotman, T., Furnari, M., & Shephard, K. (2015). Who teaches academic integrity and how do they teach it? *Higher Education*, 69(3), 435–448. doi:10.1007/10734-014-9784-3

Mail Fraud Act 18 U.S.C. § 1341 (1909)

Manly, T. S., Leonard, L. N., & Riemenschneider, C. K. (2014). Academic integrity in the information age: Virtues of respect and responsibility. *Journal of Business Ethics*, 127(3), 579–590. doi:10.1007/10551-014-2060-8

Marsh, C. (2011). Business executives' perceptions of ethical leadership and its development. *Journal of Business Ethics*, 114(3), 565–582. doi:10.1007/10551-012-1366-7

McCabe, D. L., Treviño, L. K., & Butterfield, K. D. (2001). Cheating in academic institutions: A decade of research. *Ethics & Behavior*, 11(3), 219–232. doi:10.1207/S15327019EB1103_2

Mercury News. (2015). *Unusual amount of cheating suspected at Stanford University*. Retrieved from <http://news.yahoo.com/unusual-amount-cheating-suspected-stanford-university-165354810.html>

Misprison of a felony 18 U.S.C. § 4 (1909)

Moten, J., Fitterer, A., Brazier, E., Leonard, J., & Brown, A. (2013). Examining online college cyber cheating methods and prevention measures. *Electronic Journal of E-Learning*, 11(2), 139–146.

Racketeer Influenced and Corrupt Organizations 18 U.S.C. § 1961-1968

Regents of the University of California. (2015). *Working to ensure academic integrity at UCSD*. Retrieved from <https://students.ucsd.edu/academics/academic-integrity/index.html>

Sarita, R. D. (2015). Academic cheating among students: Pressure of parents and teachers. *International Journal of Applied Research*, 1(10), 793–797.

Seals, M., Hammons, J. O., & Mamiseishvili, K. (2014). Teaching assistants' preparation for, attitudes towards, and experiences with academic dishonesty: Lessons learned. *International Journal on Teaching and Learning in Higher Education*, 26(1), 26–36. Retrieved from <http://search.proquest.com.ezproxylocal.library.nova.edu/docview/1651859266?accountid=6579>

Smithee, M. (2009). Applying cultural concepts to academic integrity. In T. Twomey, H. White, & K. Sagendorl (Eds.), *Pedagogy, not policing: Positive approaches to academic integrity at the university* (pp. 125–134). Retrieved from http://www.academia.edu/271459/Applying_Intercultural_Concepts_to_Academic_Integrity

Special English, V. O. A. (2014, September 27). *Studying in America-31-essay mills-plagiarism* [Video file]. Retrieved from <https://www.youtube.com/watch?v=98zHYdGb-T4>

The Center for Academic Integrity. (1999). *The fundamental values of academic integrity*. Retrieved from <http://www.academicintegrity.org/icaai/assets/FVProject.pdf>

Theoharis, M. (2015). *Laws on federal fraud*. Retrieved from <http://www.criminaldefenselawyer.com/crime-penalties/federal/federal-fraud.htm>

Tomar, D. (2012). *The shadow scholar: How I made a living helping college kids cheat*. New York, NY: Bloomsbury.

Trenholm, S. (2007). A review of cheating in fully asynchronous online courses: A math or fact-based course perspective. *Journal of Educational Technology Systems*, 35(3), 281–300. doi:10.2190/Y78L-H21X-241N-7Q02

Walker, M., & Townly, C. (2012). Contract cheating: A new challenge for academic honesty? *Journal of Academic Ethics*, 10(1), 27–44. doi:10.1007/10805-012-9150-y

Wallace, M. J., & Newton, P. M. (2014). Turnaround time and market capacity in contract cheating. *Educational Studies*, 40(2), 233–236. doi:10.1080/03055698.2014.889597

Weber-Wulff, D. (2014). *False feathers: A perspective on academic plagiarism*. Berlin, Germany: Springer Science+Business Media. doi:10.1007/978-3-642-39961-9

Williams, J. A. (2008). *Counterfeiting of goods: The risks and links to terrorist funding*. Retrieved from <http://www.osi.com.ph/wp-content/uploads/Counterfeiting-Links-to-Terrorist-Funding-Article.pdf>

Zicari, P. (2008). *Students admit lying, cheating, stealing to ethics survey*. Retrieved from https://www.cleveland.com/nation/index.ssf/2008/12/students_admit_lying_cheating.html

ADDITIONAL READING

Biswas, A. E. (2013). Whose code of conduct matters most? Examining the link between academic integrity and student development. *Journal of College and Character*, 14(3), 267–273. doi:10.1515/jcc-2013-0034

Brent, E., & Atkisson, C. (2011). Accounting for cheating: An evolving theory and emergent themes. *Research in Higher Education*, 52(6), 640–658. doi:10.1007/11162-010-9212-1

Bretag, T. (2013). Challenges in addressing plagiarism in education. *PLoS Medicine*, 10(12), e1001574. doi:10.1371/journal.pmed.1001574 PMID:24391477

Hrabak, M., Vujaklija, A., Vodopivec, I., Hren, D., Marušia, M., & Marušia, A. (2004). Academic misconduct among medical students in a post-communist country. *Medical Education*, 38(3), 276–285. doi:10.1111/j.1365-2923.2004.01766.x PMID:14996337

Jeffreys, B., & Main, E. (2018). *The YouTube stars being paid to sell cheating*. Retrieved from <https://www.bbc.com/news/education-43956001>

Karabag, S. F., & Berggren, C. (2012). Retraction, dishonesty and plagiarism: Analysis of a crucial issue for academic publishing, and the inadequate responses from leading. *Journal of Applied Economics and Business Research*, 2(3), 172–183.

Kumar, P. M., Priya, N. S., Musalaiah, S. V. V. S., & Nagasree, M. (2014). Knowing and avoiding plagiarism during scientific writing. *Annals of Medical and Health Sciences Research*, 4(9Suppl 3), S193–S198. doi:10.4103/2141-9248.141957 PMID:25364588

Smith, D. (2011). The diversity imperative: Moving to the next generation. In P. G. Altbach, P. J. Gumpert, & R. O. Berdahl (Eds.), *American higher education in the twenty-first century: Social, political, and economic challenges* (pp. 465–490). Baltimore, MD: The Johns Hopkins University Press.

Spiro, J. (2011). Guided interaction as intercultural learning: Designing internationalisation into a mixed delivery teacher education programme. *Higher Education Research & Development*, 30(5), 635–646. doi:10.1080/07294360.2011.598453

Zhou, J., & Fischer, K. W. (2013). Culturally appropriate education: Insights from educational Neuroscience. *Mind, Brain and Education: the Official Journal of the International Mind, Brain, and Education Society*, 7(4), 225–231. doi:10.1111/mbe.12030

KEY TERMS AND DEFINITIONS

Academic Cheating: An individual who does not utilize their own intelligence to give their interpretation of the content.

Cybercriminals: Individuals who commit crimes via the internet.

Fraud: A practice or series of acts that are designed to take advantage of individuals, systems, or other process for the benefit of someone else.

Ghostwriters: Individuals who conceal their true identities from detection by engaging in schemes intended to defraud.

Integrity: Being whole and having a consistent set of ethical, moral, and legal practices.

Paper Mills: Business entities created for the sole purpose for selling scholarly works and publications written by ghostwriters.

Plagiarism: Individuals who intentionally create and publish false information to gain an advantage or benefit.

Modus Operandi in Cybercrime

1

Bettina Pospisil <https://orcid.org/0000-0002-8854-9764>*Danube University Krems, Austria***Edith Huber** <https://orcid.org/0000-0003-3373-0870>*Danube University Krems, Austria***Gerald Quirchmayr***University of Vienna, Austria***Walter Seboeck***Danube University Krems, Austria*

INTRODUCTION

Every person has their own way of doing something, from simple-to-interpret routinized actions to significant acts, which are difficult to observe. Even though we are not aware of it most of the time, we often recognize our counterparts opposite because of their *modus operandi* before we can see their face. This “particular way or method of doing something” (English Oxford Living Dictionaries, n.d.) is called the *modus operandi*. Behind this term lies a vast and heterogeneous field of definitions and interpretations. Especially in the context of crime studies, the *modus operandi* represents an important concept to learn about offenders. This concept is used to raise the existing knowledge about the defendant and his/her approach to criminal activity, in order to predict, prevent and deter future crimes. While analysing the *modus operandi* is already well-established practice used to detect offenders in traditional forms of crime, it is not yet commonly used in cybercrime. The most important reason is the lack of insight into the approach of a cybercriminal. His/her playground is cyberspace, where it is difficult to gather all the details needed to construct a complete picture of a *modus operandi*. This difficulty arises because not all data in cyberspace is easily accessible, and even criminals with basic technical knowledge can hide themselves and camouflage their activities without much of a problem. Hence, this lack of insight leads to a lack of knowledge about the activities perpetrated before the victim recognizes the damage.

In this article the concept of *modus operandi* will be discussed within the context of the phenomenon of cybercrime. In the first chapter, the terms cybercrime and *modus operandi* will be defined. In the second chapter, the article will explore the nature of cybercrime as a topic situated at the interface of different disciplines. In particular, the challenges and topics of the three most important disciplines will be outlined. When talking about the idea of *modus operandi* in the context of cybercrime, technical aspects that represent the framework conditions warrant further consideration. The third chapter of the article will examine these in two steps. First, the technical aspects of the *modus operandi* concept in cybercrime will be set down. Next, different classifications of potential criminals will be discussed

DOI: 10.4018/978-1-5225-9715-5.ch013

and one classification type selected as an example of how the *modus operandi* in cybercrime could be analysed. In the closing chapter, the authors make recommendations concerning the need for greater awareness, knowledge, prosecution, and cooperation, and argue for the necessity of future research.

One of the objectives of this article is (1) to illustrate that valid definitions of cybercrime and of the *modus operandi* have to take the interdisciplinary nature of both concepts into account. The second objective is (2) to highlight the issues and challenges the various disciplines have to face when talking about cybercrime. This article will continue (3) with an explanation of what a *modus operandi* in cybercrime could look like in practice. This will be achieved through the use of different studies that developed a classification of the motivation of cybercriminals, with a focus being on a recent study of defendants in Austria. Last but not least, the aim of this article is (4) to present recommendations and a conclusion pertaining to the key issues to be kept in mind when talking about the *modus operandi* in cybercrime.

BACKGROUND

Before addressing the topic in more detail, the basic terms of this article, namely “cybercrime” and “*modus operandi*” will be defined as follows.

Defining Cybercrime

Researchers from all disciplines commonly understand cybercrime as a sort of crime that involves, uses or is related to the computer or to information technology (Furnell, 2003; Varghese, 2016; Wilson, 2008). “Cybercrime differs from crime primarily in the way it is committed: Criminals use guns, whereas cybercriminals use computer technology.” (Brenner, 2010, p. 10)

The most basic distinction in defining cybercrime can be made by splitting it in two categories, “computer-assisted cybercrime” and “computer-focused cybercrime” (Furnell, 2001). This distinction has been made by various researchers from different disciplines. While Furnell (2001) characterizes the terms as already mentioned, Gordon and Ford (2006) critically discuss “Type I” and “Type II” cybercrime. McGuire and Dowling (2013) call their categories “cyber-dependent crime” and “cyber-enabled crime”. The United Nations (2000) makes the distinction between “cybercrime in a narrower sense” and “cybercrime in a broader sense”, while also conveying the same core meaning as the terms used before.

1. Computer-focused cybercrime, Type I cybercrime, cyber-dependent crime, cybercrime in a narrower sense:

This type of cybercrime relates to offences that can only be committed online. These offences do not exist offline in any way; they occur within the confines of cyberspace. This type of cybercrime includes the violation of confidentiality, integrity and availability of networks, as well as of devices, data and services connected within these networks. Examples for this type of cybercrime range from the spreading of malware to hacking, and attacks on network infrastructure or websites.

2. Computer-assisted cybercrime, Type II cybercrime, cyber-enabled crime, cybercrime in a broader sense:

Cyber-enabled crime refers to cybercrime in a broader sense therefore extending the definition to include traditional offences which have moved from real life to cyberspace. These offences have existed long before cyberspace itself, but have increased in terms of their scale or reach when perpetrated in cyberspace. Typical examples of cyber-enabled crimes are fraud (such as phishing or online banking frauds), theft (especially identity-theft), virtual sexual offences against children, and cyberstalking.

Psychologists Kirwan and Power (2013) have suggested the existence of a third type of cybercrime, the so-called “crimes in virtual world”. This term refers to events that happen between online virtual characters like avatars, and constitute acts that would be counted as criminal offences in the offline world. Examples include murder, theft, sexual assault or physical violence. They moreover suggest another nuance to the definition of cybercrime, relating to the objective of the attack. They differentiate cybercrime into “property crime”, like identity theft and fraud, and “cybercrime against the person”, for example cybercrime involving the sexual abuse of children. This enhancement is similar to the one made by Clough (2015), who discusses cybercrime from a legal perspective and makes a distinction between different offences based on whether the computer is the target, if the offences are fraud-related, content-related (e.g. child pornography), or offences against the person. While the category computer as target is directly comparable with the computer-focused cybercrime, the existence of other categories implies the need for a more detailed classification of computer-assisted cybercrime.

Defining Modus Operandi

The “English Oxford Living Dictionaries” define the term *modus operandi* as “a particular way or method of doing something”, stating that “every killer has his own special *modus operandi*” (English Oxford Living Dictionaries, n.d.). Further, the Merriam Webster Dictionary refers to the concept as “a method of procedure” or especially: “a distinct pattern or method of operation that indicates or suggests the work of a single criminal in more than one crime” (Dictionary by Merriam-Webster, n.d.). The well-known sociologist Pierre Bourdieu (1976) coined the term “*modus operandi*” as part of his Habitus concept. He understood the *modus operandi* as generation principle of the Habitus, whereby the term therefore implies the constituent structures which cause the habitual structures. The *modus operandi* can therefore be seen as the guiding principle according to which forms of practice and schemes are created. However, an observing scientist can only perceive and analyse the results from evaluations and from thinking schemes: the “opus operatum”. Here, the *modus operandi* remains hidden. According to Bourdieu, however, scientific analysis must go further and try to understand the production principle of practice - the *modus operandi* - apart from the empirical observation of the products. Following Bourdieu, researchers from different disciplines tried to define *modus operandi* (De Wet, Labuschagne & Chiroro, 2009; Hazelwood & Warren, 2003; Bennell & Jones, 2005). In most cases, these researchers discuss an offender’s *modus operandi* in the context of traditional crimes like burglary and rape. The *modus operandi* concept is therefore often employed as a means of linking crimes based on behavioural information as alternative to physical evidence (Bennell & Jones, 2005).

The concept of *modus operandi* in relation to cybercrime describes the perpetrator’s approach to committing a cybercrime offence. This includes the consideration and planning of a crime in advance, as well as actual preparations, and all stages of the crime and post-processing such as the removal, concealment and blurring of traces. The identification, documentation and analysis of the *modus operandi* behind criminal activities in cyberspace is therefore of central significance to understand how cybercrime works and which principles it follows. This includes the identification of goals, targets, motivation and attack patterns as they unfold. Casey (2008) and Turvey (2011) are some of the first researchers to discuss the

relationship between the concept of *modus operandi* and technology. They mention that computer and internet-related technologies are used in different stages of criminal activities and therefore need closer analysis. Moreover, they also discuss methods by which technology could support the determination of a *modus operandi* in traditional crime cases. Some authors have already created different typologies of cybercriminals, based on their *modus operandi* (Casey, 2008; Furnell, 2001; Ngafeeson, 2010; Turvey, 2011). These categorizations differ in their focus between technical issues, the victim, motivation and objective of the offender and further distinguishing factors.

A TRANSDISCIPLINARY PHENOMENON

Cybercrime is a phenomenon that is located at the intersection of different disciplines. On the one hand (1) cybercrime on its own is an in-depth technical topic concerned with objectives as well as the approach taken of cybercrime. Moreover, cybercrime is (2) a crime against the law and therefore the topic is of great legal and criminological importance. Additionally, cybercrime is (3) a consequence of the relocation of our living space into cyberspace and the associated influence this has had on our actions - thus a social or sociological topic. With a special focus on the *modus operandi* in cybercrime, we need to bear in mind the influence of several other disciplines, i.e. media studies, psychology and economic while analysing offenders and victim's behaviour. This diversity across such a variety of disciplines clearly results in the necessity of a transdisciplinary approach in dealing with the phenomenon of cybercrime. In this section a short insight into the basics of the three most fundamental disciplines when talking about cybercrime will be given. The section will show the common concepts and challenges of these disciplines.

Technical Studies

Several institutions and agencies have tried to develop specific classifications of cybercrime from a more technical perspective, for example the Computer Security Institute (2001) and Europol (2018). While such classification attempts are valuable and necessary, rapidly developing new and disruptive technologies lead to this becoming a moving target. With every new technology come new ways of exploiting it and new approaches for countering these methods have to be developed. Therefore, a more fundamental approach, aimed at identifying the general method of attack applied by cyber criminals, is required. The Cyber Kill Chain® framework developed as part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity by Hutchins, Cloppert and Amin (2010) is a good example of documenting the approach of the offender from a technologically oriented process perspective, including possible counter measures. While this model is primarily aimed at combating advanced persistent threats, it can serve as template for dealing with cyber-attacks that are more sophisticated.

While in the past cyber-attacks depended on a criminal having a certain level of knowledge, this barrier has been considerably lowered by cybercrime now being offered as service (otherwise known as CaaS). Worrying analyses documented in the latest report from the Internet Organised Crime Threat Assessment (Europol, 2018) point towards an increasing “upstream trend”, i.e. cybercrime tools being offered as CaaS turning into a significant problem. The most worrying trend on the horizon is the ease of availability of military grade attack technology to criminals, which might soon include such advanced components as big data analysis or artificial intelligence modules for planning and carrying out cybercrime. Depending on the accessibility of technology for cyber criminals, their approach will continue to adapt and evolve,

as could already be seen during the different waves of ransomware attacks in spring and summer 2017 (Europol, 2018). A current strategy to defend against advanced forms of attacks is the concept of cyber threat information sharing: “Threat information is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor.” (Johnson et al., 2016, p. 2) According to Johnson et al. (2016) there are different types of threat information including indicators of compromise (IOCs) as well as tactics, techniques, and procedures (TTPs) used by threat actors, security alerts, threat intelligence reports and recommendations for tool configurations. To gather this information about the threat, it is necessary to scan potentially affected systems for the presence of unusual artifacts (software and data) and to detect unusual system behaviour (i.e. IOCs). That is why a significant step forward is expected from the introduction of machine learning and artificial intelligence techniques when it comes to the detection and identification of IOCs and associated emerging patterns that characterize certain forms of cyber-attacks. Burnap et al. (2017) for example used machine activity metrics with the aim to distinguish between malicious and trusted software samples. By doing so, they developed a new classification method using self-organizing feature maps.

Law and Crime Studies

“*Modus operandi* is a characteristic pattern of methods of a repeated criminal act, used to identify the culprit.” (US Legal, n.d.) This definition already shows the greatest challenge for the law studies regarding an international view on the topic cybercrime: The question of what a criminal act is will be answered very differently depending on the jurisdiction and cultural background of a person, and also the context of an action in cyberspace. The process of prosecution is additionally more complex because of different topics such as the problem of handling digital evidence and the security vs. privacy debate, to list some of the core issues. In general, legal scholars – when talking about the phenomenon of cybercrime – focus primarily on discussing national and international strategies and legislation regarding cybercrime.

In recent years, a great majority of nations have introduced a cybersecurity strategy, which can be looked up on the website of the NATO Cooperative Cyber Defence Center of Excellence (2015). Based on these strategies, a comparative analysis has disclosed six principles that can be found in all security strategies: Maintenance of existing fundamental rights and national values, disclosure of responsibilities and legal framework conditions, establishment of security and resilience of ICT systems, promotion of national and international cooperation and coordination, raising awareness and skills as well as promoting research and development, securing economic success and advantages (Pospisil, Gusenbauer, Huber, & Hellwig, 2017). The principle “disclosure of responsibilities and legal framework conditions” shows the great importance of this topic for nearly all nations. Major players like the USA (The White House, 2011), the EU (European Commission, 2013) and the United Kingdom (Cabinet Office, 2011) highlight the necessity for international prosecution and the international harmonization of the law with regard to cybercrime. Therefore, the Convention on Cybercrime (Council of Europe, 2001) constituted a significant milestone, as it was the first international agreement addressing the harmonization of national law pertaining to cybercrime. Within this convention, the member states of the council of Europe and other states agreed on necessary steps to develop international legislation as well as cross-border cooperation. Nevertheless, while some nations have enacted laws specifically directed towards cybercrime, others rely on applying existing law that deals with traditional acts of crime. From a truly international perspective it could be said that 72% of all countries have legislation regarding cybercrime, 9% have a draft legislation on the topic, and 18% do not even have legislation at all (United Nations Conference on

Trade and Development, n.d.). Although the exact legal situation depends to great extent on the nation itself, nearly all try to address four problem areas that cybercrime offences have created: the protection of privacy, the prosecution of economic crimes, the protection of intellectual property and the procedural provisions to aid in the prosecution of computer crimes (Pelker, Palmer, Raia, & Agosti, 2015).

Different authors of law studies discuss legal issues pertaining to cybercrime with a national focus. While Cartwright (2016) discusses the complicated nature of cyberspace, which is both a public and private space, Brenner (2004) concludes that the United States federal cybercrime law needs more provisions to protect the privacy of individuals. Moreover, the difficulties inherent in investigating cybercrime are numerous, and range from the national as well as international consistency of legislation, investigation and prosecution (Mohammed, Mohammed, & Solanke, 2019; Haase, 2013) to the complexity and volatility of digital evidence (Schwerha, 2004). Carter (1995), an US-based researcher, provides recommendations to improve law enforcement, which could also suit various other states “Protocols must be developed for law enforcement that address [sic] the various categories of computer crime. Investigators must know the materials to search and seize the electronic evidence to recover, and the chain of custody to maintain.” (Carter, 1995, p. 26)

Sociology

While technical studies focus on the “cyber” element of cybercrime, and legal studies on “crime”, sociology focusses on the societal factors involved in cybercrime. From a sociological perspective cyberspace basically is - to concur with Schütz and Luckmann (2003) - an expansion of the “Lebenswelt”. The “Lebenswelt”, a complex concept first introduced by Edmund Husserl (1976) and elaborated by Schütz and Luckmann, refers to the totality of the possible horizon of experience of the members of the society. As the offline world is supplemented by the online world, numerous new platforms emerge, each of them having their own norms, values and forms of behaviour (Geser, 2002). In the context of these new spaces, Geser (2002) talks about “vireality”; the phenomenon whereby the “real” character of an individual may be more genuinely expressed in its “virtual” role than in its real-world identity.

Sociologists commonly gain knowledge related to offenders, victims and attack-types as well as about prevention, technology assessment and long-term consequences. The major challenges they face are the anonymity of the cybercrime offender and the large number of cyberattacks that remain undetected or unreported. Broadhurst et al. (2013) analyses the role of organized crime groups in cybercrime. They illustrate three different types of groups: Type I – these groups operate essentially online, Type II – these groups combine online and offline offending, Type III – these groups operate commonly offline with the support of online technology. With reference to the victims of cybercrime, it is possible to talk about two major types: private persons and institutions (Huber et al., 2018). While private persons often become victims because of the exploitation of a trust relationship, institutions are often victimised due to the exploitation of a technical vulnerability. Varghese (2016) however creates a classification of 13 different types of cybercrime offences. Some of them, for example hacking and cyberstalking, receive focused attention from other researchers in the field of social science. Jordan and Taylor (1998) try an early characterization of a hacker by discussing specific principles. Their aim is to question the current picture of a hacker. Another facet of cybercrime is the phenomenon of cyberstalking. This is the obsessive harassment or threat via digital media, which has increased in recent years. More and more private individuals are becoming victims of digital acts of revenge. These can be carried out by private or professional perpetrators (Huber, 2013).

Various researchers from social science (Ogbuaja, 2016; Seböck & Pospisil, 2016; Varghese, 2016) speak out for the necessity to raise the societal awareness of cybersecurity and cybercrime, including an expansion of training programs regarding these topics.

MODUS OPERANDI IN CYBERCRIME

Technical Aspects

Cybercrime depends on the exploitation of vulnerabilities in an organization's or a person's ICT system. While attacks might first become visible through social engineering, i.e. the exploitation of human weaknesses, the actual cybercrime starts well before with a target reconnaissance phase. Whether aimed at obstruction, distortion, destruction, espionage or extortion as the preeminent goal of the cyber-criminal, planning the crime and collecting information about the victim is usually the first step, which is definitely helped by a wide range of information being available on social media, through search engines, and ultimately through web services operated by criminals. While in the past this required considerable effort, the emergence of the so called crime as a service (CaaS) has led to this and further steps of a criminal operation being offered in a way similar to web services through online market places operated by criminals who produce or modify software tools and offer to carry out cybercrime in the form of a pay-per-use-service. Worrying reports (GovCERT.ch, 2016) indicate that there are basically three major phases in an advanced cybercriminal operation: the initial target evaluation and target reconnaissance, the attack planning and weaponisation phase, followed by the actual infiltration and attack delivery. New technological developments, primarily artificial intelligence and big data analytics might soon be added to the already existing set of attack tools. While effective countermeasures are available against malware, ransomware, denial of service and some forms of advance persistent threats, the combination of these attacks with the new technological capabilities will render them far harder to prevent and counter. With regard to the already high sophistication of CaaS and emerging technological trends, it can therefore also be assumed that the defence against cybercrime must start from a comparatively high level, such as the Cyber Kill Chain® framework (Hutchins, Cloppert & Amin, 2010), which has become a standard reference since its introduction. Technology becomes increasingly sophisticated and powerful and so does its vulnerability, as can be seen in the case of IoT. Old forms of attacks will therefore also continue to exist, trying to make use of new vulnerabilities and exploiting new environments (Kolias, Kambourakis, Stavrou & Voas, 2017).

To gather information about the *modus operandi* of a cybercriminal it is a common method to describe his/her behaviour with the concept of tactics, techniques, and procedures (TTPs). By doing so, it is possible to determine a cybercriminal's tendency to use, for example, specific operations, attack tools or exploits (Johnson et al., 2016). The ATT&CK model (Adversarial Tactics, Techniques, and Common Knowledge) developed by MITRE 2015 goes a step further and allows for the process modelling of post-compromise adversary behaviour (Strom et al., 2017). This means, that the model focuses on the behaviour of the attacker after he/she got access to a system within a network. To do so, the model presents seven steps of action: identify behaviours, acquire data, develop analytics, develop an adversary emulation scenario, emulate threat, investigate attack and evaluate performance. Moreover, the model is open access for everyone, and hence functions as a globally accessible knowledge base.

Classification of Defendants

When analysing the *modus operandi* in cybercrime, it is common to take a closer look at the defendant regarding different variables. Thus researchers ask for the motivations of the defendant; the approach taken, as well as the way the victim is chosen and the choice of vulnerability used to enter the system. All this information helps illustrating different *modi operandi*, which can focus on a very precise type of defendants or can be more general.

Turvey (2011), for example, outlines six very general types of behaviour, each of which should cover the different types of crime offences: Power Reassurance, Power Assertive, Anger Retaliatory, Sadistic, Opportunistic and Profit Oriented. While some of these concepts sound conclusive, they seem not to suit well for the special topic of cybercrime offences. In contrast, Casey (2008) puts forward a very special classification, and differentiates eight motivational categories of critical information technology insiders: explorers, good samaritans, hackers, machiavellians, exceptions, avengers, career thieves and moles. Furnell (2001) presents seven motivations that a defendant could have: Challenge, Ego, Espionage, Ideology, Mischief, Money and Revenge. Based on these motivations he differentiates between nine types of defendants: Cyberterrorists, Cyber Warriors, Hacktivist, Malware writers, Old School, Phreakers, Samurai, Script Kiddies, Warez D00dz. When looking at these motifs, Furnell's (2001) results show significant similarities with the latest evidence-based classification developed by Huber, Pospisil and Seböck (2018) based on cybercrime offenses prosecuted at the Vienna Criminal Court between 2006 and 2016. The results of this analysis show that there are five different types of defendants, separated by their motivation: Revenge Crime, Financial Crime, Show-off Crime, Conviction Crime and Follower Crime. The analysis from Huber, Pospisil and Seböck (2018) identifies two typical patterns of cybercrime cases that could not be solved. These two patterns can be identified, as the literature suggests, in computer-assisted and computer-focused cybercrime:

- Computer-assisted cybercrime
 - Type I: Revenge crime
 - Type II: Financial crime
- Computer-focused cybercrime
 - Type III: Show-off crime
 - Type IV: Conviction crime
 - Type V: Follower crime

The types differed from each other not just in their motivation, but also in their approach, the way in which they chose their victims and the damage they caused. In the following, the motivational types will be illustrated briefly based on these variables and case examples. Before this, it has to be noted that the authors made the conscious decision to focus their data collection on general paragraphs of cybercrime. They therefore did not include special paragraphs of child pornography and hate crime or radicalization. This decision was based on the legal framework and the different paragraphs underlying these offences. While this analysis focuses on classical paragraphs of cybercrime, the study of child pornography offences and hate crimes like radicalization requires an examination of completely different paragraphs. Moreover, the authors follow the assumption that these content-related cases are very different from other cases of cybercrime. For this reason, it can also be assumed that the motives behind offences of child pornography and hate crimes differ from those mentioned here.

TYPE I: REVENGE CRIME

After a jealousy dispute, B separates from A. A is upset and wants revenge. Due to the former trust relationship, A knows the password that B uses for different online accounts. A can now access B's Facebook and email accounts without any problem. Once having accessed the accounts, A changes the password, views private data, deletes and modifies it or posts degrading texts and photos in B's name.

Defendants of the type *Revenge crime* commonly operate alone and usually do not have any substantial technical know-how. The defendants often act out of a love relationship that experienced a crisis. Thus the victim is generally a private person, and the attack a targeted one. The defendant usually takes a simple approach and uses the insider knowledge that he or she acquired in the context of the trust relationship against the victim. Veiling measures are not used. In cases of *Revenge crime*, the vulnerability is commonly the naivety and unawareness of the victim. In most of the cases, the offence is a data breach or an attack on networks. The consequences for the victim are usually mental harm and the loss of information.

TYPE II: FINANCIAL CRIME

A wants to make quick money and instructs B to construct a Trojan. Afterwards A logs into a public online chat and pretends to be a young girl searching for a boyfriend. C shows interest and the two soon start a private chat. Pretending it is a photo of "her", A sends a file to C. C opens this file, which in reality contains the Trojan. A can now – with the help of the Trojan – take over the computer in front of C's eyes and extorts C with the private data A now has access to.

Defendants of the type *Financial crime* usually operate in groups, and possess at least basic technical know-how. The approach taken is pretty simple, but the defendants also use basic cover-up measures such as wrong IP addresses to protect themselves. Usually these defendants search for an open vulnerability, so the attack is not targeted. In the cases of the type *Financial crime*, the defendant commonly has no relationship with the victim, who is in the majority of cases a private individual or a company. The vulnerability typically exploited by the defendant is the unawareness of the victim. Common mistakes include the use of very simple passwords and the free disclosure of confidential information by mail, telephone or other communication channels. As with the type *Revenge crime*, the common offences are data breaches or attacks on networks. Typical examples of such acts are phishing attacks and social engineering. After the attack, most victims suffer from financial damage, especially reinstatement costs.

TYPE III: SHOW-OFF CRIME

A is part of a hacker group. Together with some of his friends, A wants to show off his technical skills. They go through the critical infrastructure searching for vulnerabilities and finally find one in authority B. They launch a SQL injection and a Distributed Denial of Service attack on B. Thus, the group modifies and corrupts sensitive data. Finally, they post their attack- information about the vulnerability and the sensitive data - online to publicise their success.

As the case example shows, the defendants of the type *Show-off crime* commonly act in groups of more than two, and have technical skills that they want to show off. The defendants are typically younger and have a rather complex approach to cybercrime as compared to the defendants of the other motivational types. The defendants use camouflaging measures like the TOR-network or VPN-encryption to avoid

detection. The attack itself is often based on tools, but could also be a D(D)oS-attack. Nevertheless, defendants of this type usually search for vulnerabilities, which can also be done technically using a vulnerability scanner. Thus, the offence is not targeted and the defendant usually has no relationship to the victim. In most cases, the victim is an authority or a company and has to face reinstatement costs as well as the loss of reputation and information.

TYPE IV: CONVICTION CRIME

A is a member of a religious perpetrator group. The members of the group are convinced of their radical conviction and want to spread it to find new followers. A uses technical attacks to gain access to the homepage of B. After that A deletes the previous contents of B, and instead displays images of Djihad fighters with machine guns. Messages from the perpetrator group are also left in Arabic script.

Defendants of the type *Conviction crime* usually act in conjunction with accomplices who hold the same conviction, they want to spread. The complexity of the approach is very different and so is the technical know-how of the defendants. They commonly attack homepages of private persons or companies, in most cases to display radical appeals and prohibited content. Thus, the defendants of the *Conviction crime* choose their victim according to the degree of open vulnerability, and do usually not have a relationship to them. The victims suffer from the loss of information as well as the loss of reputation as result of radical content being present on their homepage.

TYPE V: FOLLOWER CRIME

A is very interested in technology and is therefore a participant in a few hacking forums. One day other participants brag about having cracked B's system and post instructions, vulnerabilities and sensitive data in the forum. A is curious and tries out the instructions. A gets access to B's email account, reads the emails and changes the password.

The offences of the type *Follower crime* need an enabler that is often found in the type Show-off crime. The defendants of this type of cybercrime either use existing information about vulnerabilities out of a lack of awareness and understanding that they are already committing a crime, or do it consciously out of curiosity. Thus, their approach is very simple and they do not need any technical know-how but have to participate in hacking forums or communities. The attack is not targeted and the defendants usually do not have a relationship with the victim, who could be anyone who was the victim of the enabler in the first place.

SOLUTIONS AND RECOMMENDATIONS

This contribution has so far shown that cybercrime and especially *modus operandi* in cybercrime, is a very diverse phenomenon that has to be considered through the lens of different disciplines and perspectives. Although the gathering of information about the *modus operandi* of offenders is a step in the right direction, there is not just one easy solution for the challenge of creating a safe and secure cyberspace. Nevertheless, some fundamental recommendations may be made:

Raising Awareness and Knowledge

As many studies show, a large number of cybercrime offences could be avoided if victims are made aware of nature of criminal activity online. Therefore, this recommendation has two main objectives: On the one hand, it is necessary to raise society's awareness, as anybody could become the victim of cybercrime, everyone should be prepared to reduce those risk factors within their control. On the other hand, to handle this complex topic, it is equally necessary to raise the knowledge people have regarding the technological, legal, and sociological aspects of this phenomenon. Therefore, it is necessary to anchor the topics cybercrime and cybersecurity in the education system (Jansen et al., 2017).

Improve Prosecution Through Knowledge and Cooperation

Connected to the first recommendation is the need to raise cybercrime conviction levels. Currently, it may be said that, in the context of the prosecution process, convictions are low as there is a huge lack of knowledge about cybercrime as a phenomenon. It is necessary to adequately train the stakeholders in this process – mainly the police, the prosecuting authority and court officials – so they are able to gain important information to support the investigation process (Huber, Pospisil, & Seböck, 2018). In order to deal with the challenge that cybercrime offences do not stop at national borders, it is also important to extend international cooperation in the investigation process (Rashkovski, Naumovski, & Naumovski, 2015). Only if the investigation is successful a case can be solved and prevention improved. Moreover, better stakeholder training would also lead to new information about the *modus operandi* of cybercriminals, gathered from empirical cases that could raise our knowledge about cybercrime as a phenomenon.

FUTURE RESEARCH IN OFFENDER BEHAVIOUR

This is the point where future research has to step in. The study of cybercrime requires more evidence-based analyses concerning the behaviour and *modus operandi* of offenders (Leukfeldt, 2017), as well as of the process of prosecution, in order to improve it. To be successful, future research groups should comprise different disciplines to enable the necessary transdisciplinary view on the topic.

Increase the Attractiveness of Being a “White Hat Hacker”

Last but not least, there is a trend developing that sees more and more talented young people choose a criminal career, and become a “black hat hacker”, over that of an IT-employee, or a “white hat hacker”. The reasons are numerous, and range from personal feelings like curiosity and boredom to the wish for power, peer-recognition and political participation (Madarie, 2017). Law enforcement agencies also have to think about possibilities to increase the attractiveness of becoming an IT-specialist.

Future Research Directions

As already mentioned, future research is going to be very important when it comes to a better understanding of cybercrime. For instance, dark field analysis could be a way to gather new information and raise the knowledge about the *modus operandi* of offenders in cybercrime. The research and application

of developments in the field of *modus operandi*, therefore, requires new methods and potentially new ways of thinking.

Future research on the *modus operandi* in cybercrime could take two directions:

1. While cybercrime is on the rise, the impact of the offences increases and affects more and more disciplines. Therefore, the topic becomes even broader and more interdisciplinary. Here research teams, in attempting to develop the topic try to cover as many disciplines as they can to illustrate this complex phenomenon. The core challenge hindering the development of platform or system in such a situation would be the lack of clarity because of the endlessness of impacted disciplines.
2. As cybercrime is at its core a technical topic, it is obvious that there is a need for tools aimed at a technical way to analyse the *modus operandi* of offenders. However, it is still an open question whether artificial intelligence combined with big data analytics will be able to deliver such a tool.

CONCLUSION

The *modus operandi* constitutes much more than just another cybercrime topic. Understanding the concept could be the key to answering the question of whether in future we will be able to strengthen the defence against the offence. Currently, there is an imbalance of power between attacker and defender, because attacking a system is always easier than keeping it safe. A better grasp of the *modus operandi* concept will make it is possible to deepen the understanding of the offender and thus improve prevention and reaction. To conclude, while much about the *modus operandi* of cybercriminals still remains in the dark, two core elements for successful cybercrime prevention may be identified: First, the recognition that fight against cybercrime affects everyone, because anyone could become a victim, and we need to realize that. Second, in order to win the fight against cybercrime, a more nuanced awareness of the way in which cybercrime works is necessary to both predict criminal use of technology, and to put in place timely preventive and forensic counter measures that protect individuals and organizations or (in an ideal case) deter potential attacks.

REFERENCES

- Bennell, C., & Jones, N. J. (2005). Between a ROC and a Hard Place: A Method for Linking Serial Burglaries by Modus Operandi. *Journal of Investigative Psychology and Offender Profiling*, 2(1), 23–41. doi:10.1002/jip.21
- Bourdieu, P. (1976). *Entwurf einer Theorie der Praxis auf der ethnologischen Grundlage der kabyliischen Gesellschaft*. Frankfurt am Main: Suhrkamp.
- Brenner, S. W. (2004). U.S. Cybercrime Law: Defining Offenses. *Information Systems Frontiers*, 6(2), 115–132. doi:10.1023/B:ISFI.0000025780.94350.79
- Brenner, S. W. (2010). *Cybercrime. Criminal Threats from Cyberspace*. Santa Barbara, CA: Greenwood Publishing Group.

- Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., & Da, C. (2013). *Crime in Cyber-space: Offenders and the Role of Organized Crime Groups*. Australian National University Cybercrime Observatory. Working Paper. Retrieved December 3, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2211842
- Burnap, P., French, R., Turner, F., & Jones, K. (2017). Malware classification using self organising feature maps and machine activity data. *Computers & Security*, 73, 399–410. doi:10.1016/j.cose.2017.11.016
- Cabinet Office. (2011). *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*. London: Crown.
- Carter, D. L. (1995). Computer Crime Categories. *Law Enforcement Bulletin, U. S. Department of Justice. Federal Bureau of Investigation*, 64(7), 21–26.
- Cartwright, B. E. (2016). Cyberbullying and Cyber Law. A Canadian Perspective. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-7. Retrieved May 15, 2019, from <https://ieeexplore.ieee.org/document/7740430/citations>
- Casey, E. (2008). Cyberpatterns: Criminal Behavior on the Internet. In B. E. Turvey (Ed.), *Criminal profiling: An introduction to behavioral evidence analysis* (3rd ed.). London: Academic Press.
- Clough, J. (2015). *Principles of Cybercrime*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9781139540803
- Computer Security Institute. (2001). *CSI/FBI 2001 Computer Crime and Security Survey*. Retrieved December 3, 2018, from <https://www.stealth-iss.com/documents/pdf/COMPSECSURVEY1.pdf>
- Council of Europe. (2001). *ETS 185 - Convention on Cybercrime, 23.XI.2001*. Retrieved May 15, 2019, from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
- De Wet, J. A., Labuschagne, G. N., & Chiroro, P. M. (2009). Offender Characteristics of the South African Male Serial Rapist: An Exploratory Study. *Acta Criminologica, Southern African Journal of Criminology*, 22(1), 37–45.
- European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: Safe and Secure Cyberspace.
- Europol. (2018). *Internet Organised Crime Threat Assessment (IOCTA) 2018*. Retrieved December 7, 2018, from https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf
- Furnell, S. (2001). The Problem of Categorising Cybercrime and Cybercriminals. *Second Australian Information Warfare and Security Conference 2001*.
- Furnell, S. (2003). Cybercrime: Vandalizing the Information Society. In *Lecture Notes in Computer Science: Vol. 2722. International Conference on Web Engineering* (pp. 8-16). Berlin: Springer.
- Geser, H. (2002). Towards a (Meta-)Sociology of the Digital Sphere. In *Sociology in Switzerland: Towards Cyber-space and Virtual Social Relations*. Retrieved December 3, 2018, from http://socio.ch/intcom/t_hgeser13.htm

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13–20. doi:10.1007/11416-006-0015-z

GovCERT.ch. (2016). *APT Case RUAG. Technical Report about the Espionage Case at RUAG*. Retrieved December 7, 2018, from https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf

Haase, A. (2013). Harmonizing Substantive Cybercrime Law through European Union Directive 2013/40/EU – From European Legislation to International Model Law? *2015 First International Conference on Anti-Cybercrime (ICACC)*, 1-6. Retrieved May 15, 2019, from <https://ieeexplore.ieee.org/document/7351931>

Hazelwood, R. R., & Warren, J. I. (2003). Linkage analysis: Modus operandi, ritual, and signature in serial sexual crime. *Aggression and Violent Behavior*, 8(6), 587–598. doi:10.1016/S1359-1789(02)00106-4

Huber, E. (2013). *Cyberstalking und Cybercrime. Kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Huber, E., Pospisil, B., Hötendorfer, W., Quirchmayr, G., Löschl, L., & Tschohl, C. (2018). *Die Cyber-Kriminellen in Wien: Eine Analyse von 2006-2016*. Krems an der Donau: Tredition.

Huber, E., Pospisil, B., & Seböck, W. (2018). *Without a Trace – Cybercrime, Who are the Offenders?* Paper presented at Conference DeepSec, Vienna, Austria.

Husserl, E. (1976). *Die Krisis der europäischen Wissenschaften und die transzendente Phänomenologie. Eine Einleitung in die phänomenologische Philosophie* (Vol. 6). Den Haag: Husserliana. doi:10.1007/978-94-010-1335-2

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2010). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. White Paper from the Lockheed Martin Corporation. Retrieved December 7, 2018, from <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>

Jansen, F., Koops, B., Lenthe, J. v., Maas, E., Planken, E., Schermer, B., . . . Verhoeven, M. (2017). Tackling Cybercrime. In *Research Agenda. The human factor in Cybercrime and Cybersecurity*, (pp. 55-64). Eleven International Publishing.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. *NIST Special Publication 800-150, Computer Security*. Retrieved May 16, 2019, from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

Jordan, T., & Taylor, P. A. (1998). Sociology of Hackers. *The Sociological Review*, 46(4), 757–781. doi:10.1111/1467-954X.00139

Kirwan, G., & Power, A. (2013). *Cybercrime: The Psychology of Online Offenders*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511843846

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *IEEE Computer*, 50(7), 80–84. doi:10.1109/MC.2017.201

Leukfeldt, R. (2017). The human factor examined: directions for future research. In *Research Agenda. The human factor in Cybercrime and Cybersecurity*, (pp. 67-75). Eleven International Publishing.

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology*, 11(1), 78–97.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Research Report 75. Retrieved December 3, 2018, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

Modus Operandi Law and Legal Definition. (n.d.). In *US Legal*. Retrieved December 3, 2018, from <https://definitions.uslegal.com/m/modus-operandi/>

Modus Operandi. (n.d.). In *Dictionary by Merriam-Webster*. Retrieved December 6, 2018, from <https://www.merriam-webster.com/dictionary/modus%20operandi>

Modus Operandi. (n.d.). In *English Oxford Living Dictionaries*. Retrieved December 6, 2018, from https://en.oxforddictionaries.com/definition/modus_operandi

Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(1), 56–63.

NATO Cooperative Cyber Defence Centre of Excellence. (2015). *Cyber Security Strategy Documents*. Retrieved December 3, 2018 from <https://ccdcoe.org/strategies-policies.html>

Ngafeeson, M. (2010). *Cybercrime classification: a motivational model*. Paper presented at the South-west Decision, Sciences Institute Conference. Retrieved December 3, 2018, from http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf

Ogbuaja, F. M. (2016). Sociological and technological factors that enhance cybercrime and cyber security in Nigeria. *International Journal of Law and Legal Studies*, 4(5), 207–216.

Pelker, C., Palmer, A., Raia, B., & Agosti, J. (2015). Computer Crimes. *The American Criminal Law Review*, 52(4), 793–850.

Pospisil, B., Gusenbauer, M., Huber, E., & Hellwig, O. (2017). Cyber-Sicherheitsstrategien – Umsetzung von Zielen durch Kooperation. *Datenschutz und Datensicherheit*, 628–632.

Rashkovski, D., Naumovski, V., & Naumovski, G. (2015). Cybercrime Tendencies and Legislation in the Republic of Macedonia. *European Journal on Criminal Policy and Research*, 22, 127–151.

Schütz, A., & Luckmann, T. (2003). *Strukturen der Lebenswelt*. Konstanz: UVK.

Schwerha, J. IV. (2004). Cybercrime: Legal Standards Governing the Collection of Digital Evidence. *Information Systems Frontiers*, 6(2), 133–151. doi:10.1023/B:ISFI.0000025782.13582.87

Seböck, W., & Pospisil, B. (2017). The main societal risks an automated future constitutes. *Proceedings of 25th International Scientific Conference on Economic and Social Development - XVII International Social Congress (ISC-2017)*.

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., . . . Wolf, R. D. (2017). *Finding Cyber Threats with ATT&CK-Based Analytics*. MTR170202 MITRE Technical Report. Retrieved May 16, 2019, from <https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf>

The White House. (2011). *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*. Author.

Turvey, B. E. (2011). Modus Operandi, Motive, and Technology. In *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Amsterdam: Elsevier.

United Nations. (2000). *Crimes related to computer networks*. Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Retrieved December 6, 2018, from https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf

United Nations Conference on Trade and Development. (n.d.). *Cybercrime Legislation Worldwide*. Retrieved December 6, 2018, from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

Varghese, G. (2016). A sociological study of different types of cyber crime. *International Journal of Social Science and Humanities Research*, 4(4), 599–607.

Wilson, C. (2008). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service – Report for Congress. Retrieved December 3, 2018, from <https://fas.org/sgp/crs/terror/RL32114.pdf>

ADDITIONAL READING

Brenner, S. W. (2001). *Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law*. Retrieved 7 December 2018, from <http://unpan1.un.org/intradoc/groups/public/documents/APC-ITY/UNPAN003073.pdf>

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Third Edition. Amsterdam et al.: Elsevier.

Gragido, W. (2013). Understanding Indicators of Compromise (IOC). Part I. Retrieved December 7, 2018, from <http://blogs.rsa.com/will-gragido/understanding-indicators-of-compromise-ioc-part-i/>

Higgins, G. (2010). *Cybercrime: An Introduction to an Emerging Phenomenon*. New York: McGraw-Hill Publishing.

Jacobson, H., & Green, R. (2002). Computer crimes. *The American Criminal Law Review*, 39, 273–325.

Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Florida: Taylor and Francis Group. doi:10.1201/9781420028379

Rajput, B. (2018). Understanding Modus Operandi of the cyber economic crime from people-process-technology framework's perspective. [JETIR]. *Journal of Emerging Technologies and Innovative Research*, 5(3), 1089–1094.

Turvey, B. E. (2008). *Criminal profiling: An introduction to behavioral evidence analysis* (3rd ed.). San Diego, CA: Academic Press.

United Nations Office on Drugs and Crime. (n.d.). *Repository Cybercrime. Database of Legislation*. Retrieved December 6, 2018, from <https://sherloc.unodc.org/cld/v3/cybrepo/legdb/index.html?lng=en>

1

Yadav, T., & Rao, A. M. (2015). Technical Aspects of Cyber Kill Chain. In J. Abawajy, S. Mukherjea, S. Thampi, & A. Ruiz-Martínez (Eds.), *Security in Computing and Communications. SSCC 2015. Communications in Computer and Information Science*, 536. Springer. doi:10.1007/978-3-319-22915-7_40

Necessity of Paradigm Shift in Criminological Theorizing: An Empirical Approach to the Changing Trend in Cyber Crime–Education Nexus

Ajibade Ebenezer Jegede

Covenant University, Nigeria

Olusola Oyero

 <https://orcid.org/0000-0001-7795-5516>

Covenant University, Nigeria

Nelson Okorie

Covenant University, Nigeria

Caleb Abiodun Ayedun

Covenant University, Nigeria

Mofoluwake Ajayi

Covenant University, Nigeria

INTRODUCTION

The triad of education, human development and socio-economic transformation or otherwise is central to the understanding of the processes involved in the workings of modern society. Inadvertently, the cyclical relationship existing between these three has been documented in research (Virginia, 2005; 27). Of recent, education was described as one of the accelerators of human, social and economic development (Ifenkwe, 2013:007). The importance of education remains unquantifiable across major indices of socio-economic development. Fundamentally, education promotes mastery of some certain procedures to the point where they become unconscious and automatic, it also permits the application of the procedures to structure information into conceptual knowledge that is used consciously and deliberately (Abadzi, 2006). These attributes when put together make education unique in its contributions to relational advancement globally.

Traditionally, education serves as a potent instrument for eliciting conformism to institutional rules and regulations and men in their various classes are socialized with the view of sustaining social stability and progress. However, in modern society, a subset of deliberate educational application tilts towards the retardation of development in the context of actions that are inimical to the overall interest of the generality. Few occurrences in the technological age attest to the fact that educational application is not uni-lineal in its consequences for socio-economic development. Of a truth, there is a dual application of educational inputs and with its negative connotations unabatedly becoming registerable in crime and in

a gamut of other anti-social behaviours globally. The manifest function of education that is commonly ushering and sustaining this turn of event is not farfetched. At inception, the defect of working against the interest of significant individuals and favouring few others has been the bane of education. This was aptly described by Coffey (2001) as differential outcomes of education.

In educational acquisition, the key democratic ideals of liberty and equality have always been in conflict in a nation with acute capitalist acumen (Brantlinger, 2007). Explaining this in a concise manner, Deleuze and Guattari (1983) disclosed that the emergence of monopoly capitalism radically transformed the social world: it swept away traditional social forms, as economic forces bite deeply into the symbolic textures of society itself (cited in Elliot, 2014:255). This symptom of destabilization then became recordable in the negativity attendant to educational skill utilization. Noblit and Pink (1995) argue that whereas the original philosophy for schooling hinges on achieving consensual relationship among diversely attributed populace, recent experiences have clearly shown that schooling is consistently promoting opposition, resistance and conflict in its consequences for societal survival. Apart from the factor located in biasness and inferiority attendant of diverse mode of knowledge dissemination according to Bourdieu, (1984), the unraveling scenario in the information technology age has now shown that school dropout is no longer sufficient reason for youth crime participation in the modern era. More significantly is the continued access of the vast majority of people to e-technology gadgets with its concomitant transformation of a relationship into virtuality.

E-relationship promotes the subtle quest for additional education enlightenment for its operability. Just as it were, more and more techno-elites have been drawn into the manipulation of the arena for both licit and illicit gains. More education now tilts to more crime involvement promoted by the increasing opportunities potentially offered by the virtual technologies and its environment. Consequently, this paper attempts to refocus attention to the changing trend in education and crime nexus. A departure from the hitherto paradigmatic leaning in criminology on less education more crime and substantial education, less or non-crime is gradually stirring one at the face (Miller, 1958; Moffitt, 1990; Farrington. 1992). Paradigm, as explained by Brown, Esbensen and Geis (2013:19) represents a tool that provides a general orientation to explaining and understanding crime as a phenomenon. With more and more of human activities booking their places in the cyberspace, so also is the increased yearnings for functional education to meet the demands of today virtual technological society across all facets of legal, semi-legal and illicit organs of the global community. Hence, the advocacy of this discourse is to cause an arousal on the changing trend in the theoretical fundamentals underpinning education and cyber-crime participation while using the evidentiary data collected from a youth study conducted in Lagos, Nigeria.

THEORETICAL FRAMEWORK

There is a gamut of issues propelling people into crime in modern society. Criminologists both in the classical and contemporary times have blamed culture, social structure and the economic system on the prevalence of crime (Conklin, 2007:149). Considering the various existed ideological variables on crime instigators therefore, two theoretical viewpoints become central to the basic argument of this research. First, Merton's social strain theory is appraised as relatively representing contemporary thinking in education-crime affinity while the classical discourse of Quetelet arouses and intensified our knowledge base on the affinal between the acquisition of qualitative education and virtual crime participation in the era of modernity. The concern of the latter remotely captures the hub of the argument of this research. Besides the philosophical leanings of both theory, their adequacy in time and space is basically reinforced by their

explicatory capacity in the technological age (or otherwise) and thus instigating the re-examination of the intellectual values of several extant theories that are mostly reducing crime events to the deficiency in educational acquisition. Currently, most hitherto known ideological landmarks across social science disciplines are confronted with the herculean task of achieving predictive exactness at the level of both intellectual, social, economic, political and canonical planes and this is as a result of the magnitude of change that has impacted the existing global society. Besides, more intriguing are the developments in the technological age that are basically challenging most hitherto existed knowledge in crime studies.

The process of economic development which paved the way to technological boom affects the nature, complexity, amount and characteristics of crime in circulation in modern society and thus querying all known boundaries of crime explanations. For instance, within the structural tradition of crime causation, the known theoretical explanation affecting education and crime involvement presents a symbiotic relationship experientially today rather than the inverse relationship formerly reported before the advent of ICT age. A notable scholar in the structuralist tradition, Merton (1938), expressed the view that the occupation of disadvantaged position in the social structure conscripts' the ability of youths in the lower-class category to achieve success through the socially approved means such as hard work, formal education and thrift. The inability to achieve success through these variables according to Merton becomes a precursor of crime. More education in this wise connotes less strain and little or no push into crime. In fact, goal displacement for individuals as a result of insufficient education becomes a potent stressor that will be followed by crime related activism. However, contrary to this initial observation, there is an unfolding scenario in recent times consistently exhuming the findings of past research and situating the findings of same as the most ideal construct needed to capture developments that are unraveling in today crime environment. This is located in the findings of a study conducted by Quetelet "Of the Development of the Propensity to Crime" (1842/2013) where he referred to crime instigators as the propensity to crime. He was the first classical criminologist to notice in France that there exists a correlation between the level of intellectual state and involvement in crime. Basically according to him, the higher or developed the intellectual state of a criminal, the more complex is his/her involvement in crime. (Complexity in this regard focusses on the manipulative capacities of would-be criminals). Criminals in this category are empowered or enabled to undertake complex criminal tasks requiring sophisticated processes, achieve more successes and capable of covering up crime leads. However, taking a skeptical look once again at this discovery, Quetelet expressed a dilemma on whether knowledge acquisition is injurious to human society. As a matter of fact, the "enlightened classes" (intellectuals, highly educated, wealthy) were hitherto presumed to possess more affluence and are less frequently under strain and without the necessity of having recourse to crime. Summarily, occupiers of this statuses were accounted as insulated from the push and pull of crime.

Experiencing a reverse order, one should rarely know that this position is rife in criminological theorizing until recent times when the world began to harvest new modes of crime. Despite the existence of this presumed chance, Quetelet, juxtaposed that affluence and educational knowledge have not an equal power in subduing the fire of the passions and sentiments commonly found among humans which is basically conditioning man toward hatred, greed, self-centeredness and vengeance. In a way, the acquisition of more education is not suppressive of human frailty in working contrary to societal morality. To support his findings, Quetelet engaged a comprehensive classification and analysis of crimes committed by several categories of suspects within nine hypothetical classes he created from the data collated in France from 1828-1829. Reporting on the result of the analysis, he pointed out the fact that those who are supposedly educated when duly compared with their counterparts who are adjudged less educated committed more crimes in relation to persons. This exposition in literature is in consonance

with the observation of this study. Borrowing from this view, therefore, it is interestingly to examine the influence of the intellectual state of the accused or suspects on the nature of crime pervading the virtual environment today, which represents a feat that is not a total departure from what was earlier identified by Quetelet. While in the traditional society, crime committed by those regarded as enlightened or knowledgeable were often dismissed as chivalry, this is no longer the case today. Then in the primitive societies, princes, knights and the Royals (purported to be educated) engaged the physical plundering of property and subjugated relatively non-enlightened citizens and folks residing within and those external to their domain through the use of wars and ideologies for the purpose of survival and amazing wealth. Conversely, the forms of technological driven crimes of modern society are more directed against persons rather than property. This dimension often imposes colossal loss on a myriad of people in the virtual environment. Attacks projected through hacking, information theft, ordered good diversions, online fraud, cyber bullying and stalking etc. are more impactful on people than the vulnerability of property emanating from property crimes. Non-virtual crimes in the traditional, agrarian or early technological society require little or no intellectual acumen for both its operationality and success. Virtual crimes are operable via the foundational structure technical knowledge and supported by depth educational acquisition of would be criminal.

Consequently, in the ICT environment supporting borderless interaction, possession of education skills helps promote both cyber fraud participation, support technical know-how needed to operate in the virtual world and correspondingly guarantees the survival of virtual criminal in the crime environment. The knowledge base of the virtual criminals can be adjudged to be dynamic and versatile when examined from the required skills needed to manipulate the virtual technologies. The only resource that confers this upon the criminal and sustains ICT related crime is education and will remain more education in its future sense. Both theories expounded in this section were found to be complimentary in shunning out ideas require to chat a new theoretical plane in cyber criminality.

LITERATURE REVIEW

In most traditional settings, education is quite central to the acquisition of positive outcomes both at the macro and micro levels of human society. While references were often made to the expected outcomes of education, only relatively few studies engage the negative effects of education on the individual, organization and society. This gap in literature, constitutes the focus of this research paper. The double-edged outcome of education resides in the pattern of educational skills utilization by its beneficiaries (Okafor, Imhonopi and Urim, 2011). It is common knowledge to know that education imparts knowledge and skills related to specific jobs and household management (Croteau and Hoynes, 2013:347). Developmental outcomes promoting affinity between education, the economy, society and life chances therefore has been accentuated in sociology literature (Coffey, 2001; Jegede, Ajayi and Allo, 2016). The trend that appears general in the discursive efforts of scholars of sociology of education involves the realities of educational experiences which carry both positive and negative connotations. At the entry point of these experiences involves the avowed requirements for certification of skills and the increased emphasis on credentialization with constraining effects on aspirations and basically founded on unequal pedestals for potential aspirers. The issue at stake revolving around the aforesaid experiences include challenges relating to access to education, ability to use resources in society and the nature of resources different people have at their disposal and under their direction (Barton and Walker, 2007). And considering the inhibitions derivable from the possession of or lack of these listed variables, several efforts have been

made to establish the relationship between class, pattern of education, accessibility to qualitative schooling, mobility and life chances. While these were viewed as a product of inequality and social divisions inherent in the structure of human population, these attributes also serve as the major determinant of behavioural participation. In this regard, the enactment of either acceptable or non-acceptable behaviours is therefore dependent on the perpetuity or quality time devoted to residing in a class by an individual or group and the class one belonged to is also a function of the quantity of educational acquisition, accessibility to higher paying employment and variability of life conditions of the affected individual or group. Class retention, immobility and behavioural component at any given instance, is often reinforced by cultural reproduction of differences and politics of identity construction attendant to educational experiences.

In recent times, risk factors such as the cloud of economic uncertainty, occupational future and the dire saturation of the labour market account significantly for the changing trends in educational outcomes globally. The devastating effect of this is much more pronounced among the youth due to their peculiarities. In terms of their characteristics, the youths are mostly acquirers of education than the old cohorts and thus exerting formidable pressure on the national economic system. They are also more vulnerable and having higher potentials for victimization in the context of the structural ill of any nation (Cho and Newhouse, 2011; Jegede, 2016). Major dislocation is therefore recordable in the area of being made redundant despite the possession of the requirements for absorption into the economy. Bell and Blanchflower (2010) were quick to report that being unemployed while young can cause permanent scars rather than temporary blemishes, and the potential for long-term damage can be more potent in a recessive economy which is a case akin to the eventful of the current area of study.

The worse scenario linkable to recessive economy is recordable and endemic in Africa and particularly in Nigeria due to the existence of weak institutions and policies that have wasted resources through unbridled official corruption and has consistently damaged living standards and inhibited development (Udoka, 2012; Ayedun, Durodola and Akinjare 2012; Ayedun, et al 2018). As a result, the massive impoverishment attendant to this national catastrophe has occasioned diversity of experiences that are affecting all facet of human life and in the process causing the classification of people into varied capacities in terms of abilities to command choice resources or goods. While few were enjoying the unfolding situation, there are so many people groaning under the burden of economic predicament and thus boxing them into low class with its attendant challenges. The combination of low class status, poor access to education and educational achievement, and inclination to participate in crime have been found to be correlated (Brown, Halsey, Lauder and Wells, 1997). Research has shown that educational experiences have a significant impact on behavioural choices. Importantly, youths who fail at school and eventually dropped out are the ones mostly assumed theoretically to likely engage in criminal behaviour. In this wise, academic performance is a significant predictor of crime and delinquency (Maguin and Loeber, 1996; Siegel and Senna, 2004:68). The philosophy behind this paradigmatic position involves the widely held notion in the academic circle that drop outs are likely to have fewer job prospects, make less money and are more likely to be unemployed (Regoli and Hewitt, 2003:284). Conventionally, therefore, educationally disadvantaged personalities were collectively viewed as having the potentials of participating, perpetrating and persisting in crime and other anti-social behaviour. (This factor is further explained in the later paragraphs of this review).

Asides from the synergy between defective education and crime, there are more concentration of scholars' attention to the evaluation of inequality and the role of cultural politics of education that are basically promoting reduction in access to education and the eventful of deteriorated lifestyles often leading to the adoption of anti-social options, this position notwithstanding, it is here advocated that a shift in factorial analysis of experiential outcomes and the atmosphere of socio-economic conditions

bearing non-anticipated consequences for human life chances be re-engaged to accommodate the unfolding convergence of increment in education credentialization and the corresponding technology crime participation which is soaring by the day. This shift is required to prove or capture how increasingly individuals and groups are coping with the complexities of educational outcomes and their attendant efforts at finding their footings in the unstable climate of economic downturn leading to the formation of diverse complex identity in our social environments. Consequently, this review section held constant the appreciation of the complexities of diverse factors promoting borderlines of acquisition and non-acquisition of education but it however engages the changing educational processes in those trends explaining educational access and crime participation in the technology age. Rather than been made explicable within the etiological notion of non-acquisition of education, this trend is more appreciated within the context of human nature.

In a sporadic manner, there is a condition present at birth that accounts for the dynamism of oscillating in-between the cycle of conformism and non-conformism to societal norms. These acquired attributes are further reinforced by a gamut of other social related factors with the economic being the epicenter of dislocations. Its effect is not restricted to a particular geographical boundary, but rather global and taking the toll on the life chances of several people. With the adverse consequences of economic downturn globally therefore, the problems associated with class immobility and incremental poverty account substantially for non-predictable outcomes that are obvious in the volume of crime activism in the age of e-technologies. Economic downturn has been defined as a significant decline in economic activity spread across the economy, lasting more than a few months, normally visible in real G.D.P, real income, employment, industrial production and wholesale retail sale (National Bureau of Economic Research, 2008). Mostly affected in this economic deterioration is the youth population who are consistently groping for relevance and survival. At the helm of economic downturn is the acute closure to economic resources that are essential to the survival quest of the affected group thereby forcing them to consider crime as one of the options that are readily available to them to ward off predatory consequences of closure. Youth's involvement in crime therefore is better explained by a lack of legitimate opportunities in the social structure (Guarino-Ghezzi and Trevino, 2005; Farrington, 1996). In essence, acute unemployment despite the acquisition of credentials needed for employability instigates negative innovative tendencies that are often culminating into diverse experimentations with illicit behaviours. Once the youths are idle, the society must of a necessity brace-up to contend with probable anti-normative conducts (Millie, 2009:62). This suggestion is in line with Farrington (2007:223) disclosure that criminal behaviour does not generally appear without warning. The presumed hub of illicit activity relatively opened to potentially vulnerable youths lies with the Internet. The Internet is full of excitement and adventure, but it is also full of danger and often provides opportunities to unknown bandits (Kowaliski, Limber and Agatston, 2012:8). As a matter of fact, the threshold of crime activism snaps when the forces that bind people to society are weakened or broken.

Similarly, few other theorists equally emphasized the economic powerlessness of youths in society or community experiencing structural closure. Youthful response follows the pattern of sub-culture of "smartness" often exemplified in cunning, conning and street sense. Youths in this category are known with too little education and IQ (Cohen, 1955; Miller, 1958; McShane and Williams III, 2007). The paradigmatic position on low education as a correlate of high risk predisposable factor for participation in delinquent and criminal behaviour is popularly known in criminological theories (Fagan and Pabon, 1990). Harlow (2003) in his study found that 68% of the state prison inmates, 50% of the Federal inmates and 60% of all inmates did not obtain their regular high school degree. This trend empirically cut across the correctional structures of most nations today. Wolfgang, Thornberry and Figlio (1987) for example

attributed 70% of offenses committed in Philadelphia to those in this category. This trend is the same for Nigeria. Farrington (1989) equally linked limited education to violent crimes affecting those in the ages 16-32 and with the accumulated convictions between ages 10 and 32, thus higher than the other category. In the same vein, Sweeten, Bushway and Parternoster (2009) reported a little consensus on the relationship between deficient schooling and delinquency. In their submission, inability to acquire requisite education makes the affected person prone to anti-social behaviour. This hinges on the fact that school dropout has a causal impact on delinquency and conversely, committing delinquent acts and other problem behaviour has a causal impact on dropping out of school. This causal relationship is said to be reciprocal rather than unidirectional.

Campbell (1990:173) extends the theoretical leaning on limited education as a precursor of crime to cover female offending. In her view, female enter into crime environment as a result of addressing many problems of their lives. Problems identified include; limited educational and occupational opportunities, subordination to men, child care responsibilities and the powerlessness of underclass membership they share with males in their communities. The female has the share of acute troubles in all known recessive economy. More recently, Hagan (2013) identifies two relationships that exist between education, crime and delinquency. First, the acquisition of higher education enhances self-esteem among its beneficiaries and second, there exist an inverse relationship between the amount of formal schooling individuals possess and the arrest rate of traditional crimes. The explanant of crime or delinquency participation or non-participation can be found in the varied accessibility to educational statuses that are opened to the possessors of education within the economic structure of modern nations. There is a significant increase in the employability of acquirers of “substantial education” while those that are “deficient” appear to be vulnerable to crime involvement (Schweinhart and Weikart, 1980).

In a contradistinction from what several literatures have reported on correlation between inability to meet up educationally and involvement in crime (MacDonald, 2007; Beinart, Anderson, Lee and Utting, 2002; Flood-Page et al, 2000; Capsi et al, 1998; Graham and Bowling, 1995), recent development clearly shows that increment in education does not necessarily curtail participation in delinquent or criminal behavior. It is a known fact that criminologists and educators have long speculated that increasing the educational achievement of young males might lower the probability that they engage in criminal activities (Moretti, 2005), findings from this current study espouses the fact that acquisition of more education is a pre-requisite to becoming successful in crime in the modern electronic environment. This research finding is supported by earlier findings (Denno, 1985; Day, Franklyn and Marshall, 1998). Majorly implicated in this criterion involves the sophistication involved in cyber technology permissible crimes. Germane to current study therefore is the necessity of acquiring education on the basis of operationality of cyber technology (most especially the Internet) which is a pre-requisite for achieving breakthrough in cyber fraud.

Method

This survey that was conducted in Lagos to unravel the causes of youth's participation in cyber fraud adopted mixed method design for data gathering. The quantitative approach identified two categories of respondents while the qualitative content was supplied through Focus Group Discussion and In-depth Interview. The latter was used to reinforce the quantitative data. The first category consists of youths residing in the general public of the study area who were assumed to be non-participants in cyber fraud activism. 1000 copies of the questionnaire “A” was administered to this group. The second category were youths suspected to be perpetrators of online fraud and was purposively accessed in diverse cyber cafés

in the selected area. 800 copies of questionnaire “B” were allotted and administered to this group. For the purpose of sampling, Lagos state was delimited into three senatorial districts forming the entirety of the state (West, East and Central districts). In line with the number of Local Government Areas in the state, (twenty in all), six Local Government Areas were used for the study. The West having ten Local Government Areas by virtue of its size was allotted four while East and Central having five each produced one each for the study. The Local Government Areas so selected were randomly selected adopting the principle of sampling without replacement. Reporting on the retrieval rate, a total of 805 copies was recovered and analyzed for those in the general public while a total of 426 were retrieved from the suspected category and processed. At the level of analysis, two hypotheses that were instrumental to knowing the role of education in online fraud activism were tested. The two featured three important variables that helped in the research effort toward ascertaining the causal factor of fraud participation on one hand and determining the level of education needed to be successful in cyber fraud business on the other hand. In relation to the qualitative methods adopted, focus group discussion (FGD) and in-depth interview (IDI) sessions were conducted. A session of FGD was conducted in Ikoyi prison in Lagos with seven participants who were mainly fraud convicts. IDI sessions comprise the engagement of two fraud convicts who disclosed their knowledge and participation in online fraud prior to their incarceration, two participants from the youths in the general public of the study and two representatives of the Economic Crime and Financial Commission (EFCC) staff accessed in Lagos and Abuja. Inputs from these respondents were analyzed in the data and analytical sections of this paper.

ANALYSIS OF PRECIPITATOR OF ONLINE FRAUD

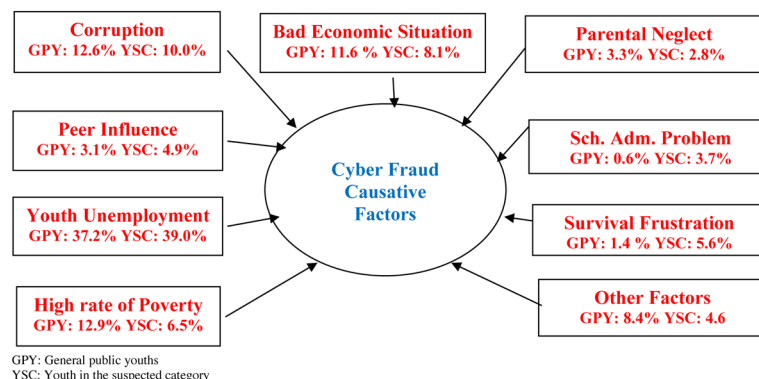
In a bid to unravel the instigators of cyber fraud with the view of knowing the explicable factor in education-crime nexus, the respondents were asked to give their opinions on the probable factors promoting cyber fraud. The responses provided by the surveyed population are depicted in the figure.

As depicted in Figure 1, 12.6% of GPY and 10.0% of YSC disclosed that the existence of corruption in Nigeria accounts for the spate of online fraud while 11.6% of GPY and 8.1% of the YSC blamed bad economic situation on the prevalence of cyber fraud. Similarly, 3.3% of GPY and 2.8% YSC viewed parental neglect of children in modern society as the probable cause of crime among the youths. Peer

Figure 1. Respondents views on the causative factors of cyber fraud in percentage

GPY: General public youths

YSC: Youth in the suspected category



influence was given as the instigator of fraud by 3.1% of GPY and 4.9% of YSC while 0.6% of GPY and 3.7% of YSC lamented that the inability of youths to secure admission into colleges to pursue higher education explains their involvement in fraud. Youth's unemployment secured a relatively large response from the two categories of respondents. 37.2% of the GPY and 39.0% of the YSC directed attention to the problem of unemployment in Nigeria as a major cause of youths –crime participation. Unemployment in this regard polled higher when compared to other factors fingered by the respondents as a probable cause of cyber-fraud. In the same vein, 1.4% of GPY and 5.6% of YSC attributed frustration attendant to survival instinct as the push factor in youth's crime participation while the high rate of poverty was seen as a vital preponderance of youth's involvement in crime by 12.9% of the GPY and 6.5% of the YSC. Finally, 8.4% of GPY and 4.6% of YSC mentioned other causes such as the defective nature of the configuration of the Internet technology, which often gives room to illegal manipulation, some viewed it as criminal conduct while few other dismissed it as youthful fun.

Summarily looking at the data, it is very clear that the amalgam of attributable factors identified by the respondents' count when situating the probable causes of cyber fraud. Yet however convincing these arguments may be, decorum demands that one should limit his/her search to at least a researchable factor. It then became compelling to zero on the effect of unemployment on youth-crime participation just as appreciable number of respondents opined that it accounts for the current situation. Apart from opinion expressed by this latter category of respondents, one should rarely draw inspiration from the old maxim which states that "idleness is the progenitor of negative inventions", hence the need to restrict the research attention to the occurrences within the borderlines of unemployment in Nigeria. As a fundamental social problem in the modern world, unemployment often pressures or impresses it upon the unemployed to engage intellectual reflection towards survival in the face of daunting circumstances. The consequences of these decisions that are attendant of pressure posed by joblessness on both learned, unlearned and other set of people which affect the ordered state of relationship in the virtual environment informs the conduct of this study. As a matter of fact, unemployment by its nature promotes a remarkable linkage between youth quest for survival, relevance and crime participation. Consequently, further effort was made to determine consequences of unemployment for increment in cyber fraud. This is done by testing the relationship between unemployment and crime.

Unemployment and Crime

Unemployment has severally been blamed on the rising rate of different types of crime in all known society. In 2009, ILO report shows that in the year 2008, with an estimated 190 million people world-wide—6 percent of the global labour force was revealed to be unemployed. Similarly, U.N.O. (2005) also espoused that globally, youths without jobs create a risk for crime, violence and political conflict. It is in view of the enormity of jobless people and its attendant risk located in crime involvement that an attempt was made to examine the contribution of unemployment to the ongoing youth's negative cyber culture. Theoretically, youths without jobs are completely fenced out from the mainstream societal goal attainment thereby suffering non-inclusion. The unemployed often experience the non-realization or dislocation of aspirational needs and are confronted with the risks of survival. This is valid from the standpoint of R. K. Merton's perspective. Therefore, in an effort at testing a relationship between the two variables of unemployment and crime, a cross tabulation was done. The examination was meant to know if unemployment among the youths has significant impact on the prevalence rate of cyber fraud on

one hand and to know if it has any effect on the decision of more educated persons to engage in crime on the other hand. To give a robust finding, the significance and the strength of relationship that exist between both was investigated through the use of chi square and phi correlation coefficient.

The cross tabulation in Table 1. Indicates that in testing the relationship between unemployment and cyber fraud involvement, 404 (100%) respondents of the YSC gave their responses, however, it was only 23.0% who agreed that there exists a correlation between unemployment and cyber fraud participation among Nigeria's youths. The Chi-Square value indicated 1.243 at p-value of 0.265 which shows a statistically significant relationship between the two variables compared.

The phi correlation coefficient was used to increase the depth of our understanding of the relationship that exists between unemployment and cyber fraud involvement. The result at a value of -0.55 shows that there is a relationship between unemployment and cyber fraud participation among the youths. In relation to the strength of association, it is very weak. This result is not quite unusual since earlier research had shown that the relationship between unemployment and crime remained unsettled and aggregate crime rates and aggregate unemployment rates seem weakly related across diverse studies in most cases. Once a youth is wrongly positioned by reason of joblessness, its attendant impact may be devastating. Association was earlier observed between family poverty (often sustained by unemployment), youth motivation, achievement and behavioral dislocation (Brook-Gunn and Duncan, 2007). Research has equally reported that those who suffer as a result of unemployment stand the risk of having no income and at the same time encountering various other difficulties (Furaker, 2009; Strandh, 2000; Alm, 2001). The existence of lack of opportunity instantiate higher crime rates and crime becomes more acute when youths have to jostle for the limited number of spaces in the job market for placement (Siegel, 2010).

Research has established a relationship between unemployment, poverty and invariably crime (D'Alessio and Stolzenberg, 2002:178; Pastrana, 2009). The economic model predicts that as opportunities—jobs—become scarce, the relative attraction of illegal activities is enhanced. And as more and more youths face stiff challenges, the tendency to source for the alternative becomes rife. It is quite obvious as few scholars have alluded to this. Rosenthal (2005) argues that "Financial pressure contributes to the incentives to create fraud. High rates of unemployment among the youths has been accentuated by research (NISER, 2007). Unemployment is a purely socio-economic problem. Rather than been construed as individual's faulty character (Especially when youths are accounted as indolents) or lack of job skills, unemployment is a public issue that results from the failure of the economic and political institutions of

Table 1. Chi-square test illustrating relationship between unemployment and cyber fraud involvement

Unemployment among Youths	Trying to get money/property		Total
	Yes	No	
Agree	85 (23.0%)	284 (77.0%)	369 (100%)
Disagree	11 (31.4%)	24 (68.6%)	35 (100%)
Total	96 (23.8%)	308 (76.2%)	404 (100%)
Chi-Square Tests	Pearson Chi-Square = 1.243		Likelihood Ratio = 1.173
Symmetric Measures		Value	Approx. Sig.
	Phi	-.055	.265
	Cramer's V	.055	.265

society to provide job opportunities to all citizens (Mooney et al, 2009). Youths are the most affected when considering the challenges of unemployment and with grave implications for socio-economic relationships (Edwards, 2009). With the downturn in the economy, the perception that the opportunity to commit fraud is there for taking, coupled with financial pressures, provide the incentive for rising level of on-line fraud and other types of crimes. The prevalence of crime among Nigeria youths draws strength from the situation of unemployment. With the existence of unemployment therefore, all road then leads to the experimentation with diverse probable alleviators in which the use of ingenuity and the application of intellectual abilities represents but one of other solvents. In this regard, the adaptation of gained educational knowledge is instantiated by the pressure posed by unemployment. Education resource in essence, creates the easy landing into the manipulation of instrumentation of fraud which is knitted with modern Internet technology. Educational knowledge assists in the youth's quest towards navigation or surfing online to access and curry to themselves electronic borne "smart" money alongside other choice goods. In an attempt at situating the processes in a clearer perspective, further examination is made to control for the relationship between education and crime.

Education and Crime Affinity

To zero in on the relationship between education and crime participation, effort was geared towards knowing the depth of relationship by testing the level of significance through the use of chi square. The phi correlation coefficient was also used to determine the strength of the relationship. Finally, the crammer's value was generated to indicate the strength of association.

The cross tabulation in Table 2. shows that in the relationship between education and cyber fraud involvement. 412 (100%) of the YSC responded to both items. 5.2% of the respondent obtained primary school leaving certificate, 28.9% were school certificate holders, 20.0% had OND/NCE certificates, 41.0% possess HND/B.Sc. degrees and 3.0% other were either professionals or would have obtained one skill or the other with or without official reckoning. This may likely include people with no formal education (popularly called illiterates). The Chi-Square value indicated 17.55 at p-value of 0.002 indicating a sta-

Table 2. Chi-square test illustrating relationship between education and cyber fraud involvement

Education	Trying to get money/property		Total
	Yes	No	
Primary	5 (38.5%)	8 (61.5%)	13 (100%)
Secondary	28 (15.6%)	152 (84.4%)	180 (100%)
OND/NCE	20(25.3%)	59 (74.7%)	79 (100%)
HND/B.Sc	41 (34.7%)	77 (65.3%)	118 (100%)
Other	3 (13.6%)	19 (86.4%)	22 (100%)
Total	97 (23.5%)	315 (76, 5%)	412 (100%)
Chi-Square Tests	Pearson Chi-Square = 17.552		Likelihood Ratio = 17.442
Symmetric Measures		Value	Approx. Sig.
	Phi	.206	.002
	Cramer's V	.206	.002

tistically significant relationship between the two variables compared. Examining this from the context of existing literature, research finding have earlier established a reciprocal relationship between the risk factor inherent in educational deficiency and the outgrowth of criminal instinct in youths cross culturally (Kraemer et al, 2001). However, this study obtained a different result. It was obtained that educational attainment forms a pre-requisite to being able to function and remained successful in cyber fraud business. This is a departure from the conventional sense explaining the preconditions to becoming criminal.

The phi correlation coefficient was deployed to test the strength of the association between the two variables. The result at a value of 0.206 showed that there is a significant relationship between education and fraud involvement. The relationship is however weak.

Crammers view intensifies our understanding of the depth of the association between education and cyber fraud involvement. The result at a value of 0.206 still reflects some degree of association between the two variables but also at a weak level. In evaluating the type of relationship that exists between education and cyber fraud involvement, it was noticed that a significant relationship exist but not strong enough to explain the reason for the current trend in youth's crime participation. Further examination was made through the use of qualitative methods to generate the potency of such relationship. This additional data gave credence to the essentiality of educational acquisition in defrauding others in the modern day online relationship.

In the data presented in Table 3, 43.9% of YSC directed attention to the immense value that educational acquisition confers on becoming an expert in cyber fraud arena. This in a way may be uncontestable when one looks at the dexterity needed to con others that are of equal intelligence as the fraudsters or better still even if not superior in knowledge to those to be conned. Research data also confirmed the additional advantages that higher educational qualifications provide to con artists in their quest to access higher and fertile opportunities in the e-business environment. 49.9% of YSC reiterated the benefits derivable in the possession of higher school certificates especially as it helps in the manipulation of sophisticated softwares that are valuable in accessing more lucrative targets such as that of institutions, industrial and governmental organizations. However, looking at this relationship from the qualitative base, there is an affinity in part and there also exists some dissension. Although, three respondents that participated in the FGD had earlier expressed skepticism about the necessity of education in the perpetration of fraud but the two other respondents with vast knowledge in on-line fraud were of the conviction that education is important to being successful in cyber fraud business. However, while the expression of skepticism came pungently in the submission of the former, it was a different case with the self-confession with another two interviewee drawn from the convicted fraudsters (though this two were not exactly convicted for cyber fraud but both have previously perpetrated cyber fraud) engaged in Ikoyi prison. Those who viewed education as unimportant to fraud success have this to say:

Respondent A. Sir, fraud may not require too much education. But I may not know if cyber fraud requires education to be successful.

Table 3. Educational factor in cyber fraud involvement (quantitative input)

Variables	Percent
	n=426
Education is important to being successful in yahoo fraud	Yes
Attainment of Higher education will confer more benefit to fraudsters.	43.9
	49.9

Respondent B. 419 people are guy man. They are not like you who have certificates. What is necessary is the right tip and you follow it up?

Respondent D. I don't know much about yahoo but I do know that education is not compulsory to operate property fraud. You needed only to be sharp, get right information on offers and be calculative.

Considering the positions of these three respondents, it is very clear that they both belonged to the category of the traditional fraudsters. The fraud professionals in this category rely to a large extent on calculative intelligence which may or may not require the application of complex technicalities demanded by the new technologically driven fraud. In the traditional context of fraud, educational acquisition is not a prerequisite. Both 'common' and 'uncommon' sense guarantee success.

But contrary to the reactions expressed above in the course of FGD exercise on the non-importance of education to being successful in online fraud, two respondents who were thought knowledgeable in the art of online fraud (drawn from the FGD respondents) were later selected for IDI and their views are recorded below:

Respondent C. In cyber fraud, you need to know how to key into the psychic of those 'mugu' (fraud victims). Operation of the Internet requires the right word and the manipulation of the right softwares. If you are not educated, how do you use 'bulk sender' software to reach out to as many people in the cyber space? How do you load your cards with the appropriate sum of money that suit your purpose? How do you know how to respond and counter all obstacles that won't allow your victims to deliver? Let me tell you, without being educated you cannot get much from yahoo. I have been into this for some times now. I am talking from experience though, yahoo crime is not what brought me to prison. It is the collection of money from people under the pretext of securing international passport for them that caused my being docked. To be truthful, I always engage the faking of such document on-line.

Respondent F. 'Yahoo boys' are in their various classes. Don't venture into yahoo if you are not adequately educated. All what you needed to operate successfully require technical knowledge on how to get across to people who will flow along with you. There are diverse area of interest you must take care of. Most importantly is your ability to conceal all the leads that can expose you to arrest and prosecution. How do you do this without having adequate knowledge in manipulating the Internet? Concealing your identity and country of operation is quite important. You may be operating in Nigeria and can as well disguise as if you are in London. There are softwares that can make you a clean impostor. What about accessing other people's bank account in various international banks? All of these requires the ability to be adequately educated. Sir, for instance, how do you trail government cheques moving from one destination to the other if you cannot manipulate a tracking software?

Analyzing the submissions of this operators or professionals in online fraud, it is glaring that robust success can only be attainable when one gets extensive education that will help any would-be criminal manipulate diverse software that make online crime robust. The immense value of education to cyber-crime cum fraud maturation cannot be underplayed. This is obvious from the reasons jointly alluded to in relation to the importance of education to cyber fraud as expressed by those who have operated this type of fraud in the past. This finding represents a point of departure from the known paradigm of what

guarantees being successful in the traditional fraud crime in particular and in most crimes in general. Several researches as often dismissed criminals or youths into crime as school drop-outs but the reverse is the case with on-line fraud for instance and for other virtual driven crime unfolding in the modern society hence the need to have a theoretical rethink on the relationship between education and crime in the criminological circle.

CONCLUSION AND RECOMMENDATIONS

It is a pre-requisite to any criminological endeavor to capture why people engage in crime activities, determine factors enhancing their choice of criminal mode and spontaneously generate a robust principle and other forms of knowledge regarding the handling of deviance and anti-social issues. This trio constitute the subject matter of this paper given the ontological status of virtual crimes. Ideally, this study captures events unraveling in the ICT arena which is unabatedly featuring a staggering number of cases of cyber related victimization basically leading into loss of resources and simultaneously heightening the status of fear in the use of e-technologies. Importantly, this paper systematically queried the veracity of the hitherto postulation regarding the inverse relationship linking crime participation and educational attainment. It was noted that the complexities attendant of the modern e-relationships that are consistently enabled by virtual technologies requires a concerted re-examination in criminology theoretical field. It is informative to know that, just as the nature and operation of crimes are changing, so also is the reduction in the capacities of existing criminological theories in comprehending its ramifications. In the cyber environment, apart from the fact that there are diverse emerging crimes that may be dismissed as “non-utilitarian” when assessed from their end results, it is glad to state emphatically that they confer satisfaction on their perpetrators and inflict injuries on diverse victims globally. Crimes such as cyber stalking, cyber bullying, cyber rape, and host other crime in the virtual environment may fall into this category. Asides from cybercrimes that were for the purpose of convenience classified as non-utilitarian in the true sense of it, there are other cyber related crime requiring unique intelligence and special intellectual capacity to operate. One may be delighted to know that those in this category command high rate of return in gains or benefits to the perpetrators. Crimes in this category is well grounded and best examined from the purview of the quantity of education at the disposal of virtual crime inducers at any given moment. This study firmly asserts that education in the modern e-environment is unavoidably important in getting economic goods in both legal and illegal activities. It permits the penetration into the realm of the unknown, confers deeper understanding of criminal tactics in reaching out to a vast majority of ICT users and thus increase their levels of victimization. This category of crime equally broadens the latitude of criminal operation into all sectors of criminal interest. This is made possible by reason of mass adoption of ICT technologies to meet domestic requirement of a myriad of people all over the world. This arena remains a platform for manifold opportunities with its flexibility in creating a convergence for both morally upright and depraved persons to operate with little or no restriction as to what their intentions may be. However, ICT environment made available its operation in unequal terms since the medium imbues those with higher educational qualification the capabilities to think haywire and to expand the web of vulnerability for other users. It is on this basis that an inward re-examination of the current theoretical assumption on “little education” higher involvement in crime and “higher

education”, minimal cases of crime participation is recommended. This option becomes expedient as more and more human interactions tend to gain their bookings in the virtual world. With this change in focus, it will equip the enforcement agencies the skill of beaming their search lights on those hitherto construed as non-infectable, or insulated in crime epidemiology. The hub of crime in the virtual era is linkable to the activities of those classified as enlightened, educated and calculative, hence there is a need for theoretical renewal and recalibration. This effort if expeditiously engaged, will aid speedy crime tracking system, usher in improvement in online related crime appreciation and increase the rate and certainty of arresting cyber implicated crimes globally.

REFERENCES

- Abadzi, H. (2006). *Efficient learning for the poor: Insights from the frontier of cognitive neuroscience*. Washington, DC: IBRD/World Bank. doi:10.1596/978-0-8213-6688-2
- Alm, S. (2001). *The Resurgence of mass unemployment. Studies of the social consequences of joblessness in Sweden in the 1990s*. Stockholm: Swedish Institute for Social Research.
- Ayedun, C.A., & Durodola, O. D., Oni, S. A., Oluwatobi, A.O., & Ikotun, O.T. (2018). The Flooding Effect on Residential Property Values: A Case Study of Shogunro Residential Estate, Agege; Lagos State Nigeria. *International Journal of Civil Engineering and Technology*, 9(6), 489–496.
- Ayedun, C. A., Durodola, O. D., & Akinjare, O. A. (2012). An Empirical Ascertainment of the Causes of Building Filure and Collapse in Nigeria. *Mediterranean Journal of Social Sciences*, 3(1), 313–323.
- Barton, L., & Walker, S. (2007). The conflict perspective: A Marxian approach. In R. Meighan & C. Harber (Eds.), *A sociology of educating* (5th ed.; pp. 316–335). New York: Continuum International Publishing Group.
- Beinatt, S., Anderson, B., Lee, S., & Utting, D. (2002). *Youth at risk? A national survey of risk factors, protective factors and problem behaviours among young people in England, Scotland and Wales*. London: Community That Cares.
- Bell, D., & Blanchflower, D. (2010). *Young people and Recession: a lost generation*. Working paper. Dartmouth College.
- Bourdieu, P. (1984). *Distinction: A social critique of the judgement of taste*. Cambridge, MA: Harvard University Press.
- Brantlinger, E. (2007). (Re) Turning to Marx to understand the unexpected anger among “winners” in schooling: A critical social psychological perspective. In *Late to class: Social class and schooling in the new economy*. Albany, NY: State University of New York Press.
- Brooks-Gunn, J., & Duncan, G. J. (2007). The effects of poverty on children. *The Future of Children*, 7, 34–39. PMID:9299837

Brown, P., Halsey, A. H., Lauder, H., & Wells, A. S. (1997). The transformation of education and society: An introduction. In A. H. Halsey, H. Lauder, P. Brown, & A. S. Wells (Eds.), *Education: culture, economy, society*. Oxford, UK: Oxford University Press.

Brown, S. E., Esbensen, F., & Geis, G. (2013). *Criminology: Explaining crime and its context* (8th ed.). Elsevier Inc.

Campbell, A. (1990). Female participation in gangs. In C. Ronald Huff (Ed.), *Gangs in America* (pp. 163–182). Newbury Park, CA: Sage Publications.

Caspi, A., Wright, B. R., Moffitt, T. E., & Silva, P. A. (1998). Early failure in the labour market: Childhood and adolescent predictors of unemployment in the transition to adulthood. *American Sociological Review*, 63(3), 424–451. doi:10.2307/2657557

Cho, Y., & Newhouse, D. (2011). *How did the great recession affect different types of workers? Evidence from 17 middle income countries*. Policy research working paper 5636. Washington, DC.: World Bank

Coffey, A. (2001). *Education and social change*. Buckingham, UK: Open University Press.

Cohen, A. K. (1955). *Delinquent boys*. Glencoe, IL: Free Press.

Conklin, J. E. (2007). *Criminology* (9th ed.). Pearson Education Inc.

Croteau, D., & Hoynes, W. (2013). *Experience sociology*. New York: McGraw-Hill Companies Inc.

D'Alessio, D., & Stolzenberg, L. (2002). A multilevel analysis of the relationship between labour surplus and pretrial incarceration. *Social Problems*, 49(2), 178–193. doi:10.1525p.2002.49.2.178

Day, H. D., Franklyn, J. M., & Marshall, J. J. (1998). Predictions of aggression in hospitalized adolescents. *The Journal of Psychology*, 132(4), 427–435. doi:10.1080/00223989809599277 PMID:9637024

Deleuze, G., & Guattari, F. (2014). Post modernity as schizoid desire cited. In A. Elliot (Ed.), *Contemporary social theory: An introduction* (2nd ed.; pp. 254–258). New York: Routledge.

Denno, D. (1985). Sociology and human developmental explanations of crime: Conflict or Consensus? *Criminology*, 23(4), 141–174. doi:10.1111/j.1745-9125.1985.tb00371.x

Edwards, K. (2009). Commencing unemployment. *Economic Policy Institute*. Available at <http://epi.org>

Fagan, J. A., & Pabon, E. (1990). Contributions of delinquency and substance use to school dropout. *Youth & Society*, 21(3), 306–354. doi:10.1177/0044118X90021003003

Farrington, D. P. (1989). Early predictors of adolescent aggression and adult violence. *Violence and Victims*, 4(2), 79–100. doi:10.1891/0886-6708.4.2.79 PMID:2487131

Farrington, D. P. (1992). Explaining the beginning, progress and ending of anti-social behaviour from birth to adulthood. In J. McCord (Ed.), *Facts, Frameworks and Forecasts: Advances in criminological theories*. New Brunswick, NJ: Transaction.

Farrington, D. P. (1996). *Understanding and Preventing Youth Crime*. York, UK: Joseph Rowntree Foundation.

Farrington, D. P. (2007). Human development and criminal career. In M. E. Vogel (Ed.), *Crime, inequality and the state*. New York: Routledge.

Flood-Page, C., Campbell, S., Harrington, V., & Miller, J. (2000). *Youth Crime: Findings from the 1998/99 Youth Lifestyles Survey. Home Office Research Study 209*. London: Home Office.

Furaker, B. (2009). Unemployment and social protection. In M. Guigni (Ed.), *Unemployment in Europe: Policy responses and policy action* (pp. 17–34). Padstow: TJ International Limited.

Graham, J., & Bowling, B. (1995). *Young People and Crime. Home Office Research Study 145*. London: Home Office. doi:10.1037/e450582008-001

Guarino-Ghezzi, S., & Travino, A. J. (2005). *Understanding crime: A multidisciplinary approach*. New Providence, NJ: Matthew Bender & Company, Inc.

Hagan, F. E. (2013). *Introduction to criminology: Theories, methods and criminal behaviour* (8th ed.). London: Sage Publications Ltd.

Harlow, C. (2003). *Education and correctional populations. Bureau of Justice Statistics Special Report*. Washington, DC: U.S. Department of Justice.

Ifenkwe, G. E. (2013). Educational development in Nigeria: Challenges and prospects in the 21st century. *Universal Journal of Education and General Studies*, 2(1), 7–14.

ILO (International Labour Office). (2009). *Global Employment Trends 2009*. Geneva: International Labour Office.

Jegede, A. E. (2016). Modern Technology, Global Risk and the Challenges of Crime in the Era of Late Modernity. In N. Okorie, B. R. Ojebuyi, & A. Salawu (Eds.), *Impact of the Media on African Socio-Economic Development* (pp. 18–32). IGI Books Publication.

Jegede, A. E., Ajayi, M. P., & Allo, T. (2016). Risk and investment decision making in technological age: A dialysis of cyber fraud complication in Nigeria. *International Journal of Cyber Criminology*, 10(1), 62–78.

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). John Wiley & Sons Ltd.

Kraemer, H., Stice, E., Kazdin, A., Offord, D., & Kupfer, D. (2001). How do risk factors work together? Mediators, moderators, and independent, overlapping, and proxy risk factors. *The American Journal of Psychiatry*, 158(6), 848–856. doi:10.1176/appi.ajp.158.6.848 PMID:11384888

MacDonald, R. (2007). Social exclusion, youth transitions and criminal careers: Five critical reflections on “risk”. In A. France & R. Homel (Eds.), *Pathways and Crime Prevention. Theory, Policy and Practice*. Cullompton: Willan Publishing.

Maguin, E., & Loeber, R. (1996). Academic performance and delinquency. In *Crime and justice: An annual review of research* (vol. 20, pp. 145–264). Chicago: University of Chicago Press.

McShane, M. D., & Williams, F. P. III. (2007). *Youth violence and delinquency: Monsters and Myths* (Vol. 1-3). Westport, CT: Greenwood Publishing Group, Inc.

Merton, R. (1938). Social structure and anomie. *American Sociological Review*, 3(5), 672–682. doi:10.2307/2084686

Miller, W. B. (1958). Lower class culture as a generating milieu of gang delinquency. *The Journal of Social Issues*, 14(3), 5–19. doi:10.1111/j.1540-4560.1958.tb01413.x

Millie, A. (2009). *Anti-social behaviour*. Open University Press.

Moffitt, T. E. (1990). The neuropsychology of juvenile delinquency: A critical review. In M. Tonry & N. Morris (Eds.), *Crime and Justice* (pp. 99–169). University of Chicago Press. doi:10.1086/449165

Mooney, A. L, Knox, D., & Schacht, C. (2009). *Understanding social problems*. Wadsworth: Cengage Learning.

Moretti, E. (2005). *Does education reduce participation in criminal activities?* National Bureau of Economic Research (NBER).

NISER (Nigerian Institute of Social and Economic Research). (2007). Report of baseline study on employment generation in the informal sector of Nigerian economy. African capacity building foundation/ international labour organization project on strengthening the labour market information and poverty monitoring system in Africa, Ibadan, Nigeria.

Noblit, G. W., & Pink, W. T. (1995). Mapping the alternative paths of the sociology of education. In W. T. Pink & G. W. Noblit (Eds.), *Continuity and contradiction: The futures of the sociology of education* (pp. 1–32). Academic Press.

Okafor, E. E., Imhonopi, D., & Urim, U. M. (2011). Utilisation of internet services and its impact on teaching and research outputs in private universities in South-Western Nigeria. *Australian Journal of Emerging Technologies and Society*, 9(2), 135–151.

Pastrana, D. (2009). *Rising unemployment and poverty in the Philippines*. Retrieved from www.wsws.otg

Quetelet, A. (2013). Of the development of the propensity to crime. In *Criminological perspective* (3rd ed.; pp. 23-39). London: SAGE Publications Ltd.

Regoli, R. M., & Hewitt, J. D. (2003). *Delinquency in Society* (5th ed.). New York: McGraw-Hill Companies, Inc.

Rosenthal, R. A. (2005). Economic and crime. In S. Guarino-Ghezzi & A. Javier Trevino (Eds.), *Understanding crime: A multidisciplinary approach* (pp. 61–90). New Providence, NJ: Matthew Bender & Company, Inc.

Schweinhart, L. J., & Weikart, D. P. (1980). *Young children grow up: The effect of the Perry preschool program on youths through age 15*. Ypsilanti, MI: High/Scope.

Siegel, L. J. (2010). *Criminology: Theories, patterns and typologies* (10th ed.). Wadsworth: Cengage Learning.

Siegel, L. J., & Senna, J. J. (2004). *Essentials of criminal justice* (4th ed.). Belmont: Wadsworth/Thompson learning.

Strandh, M. (2000). *Varying unemployment experiences? The economy and mental well-being*. Umeå University Department of Sociology.

Sweeten, G., Bushway, S. D., & Paternoster, R. (2009). Does dropping out of school mean dropping into delinquency? *Criminology*, 47(1), 47–91. doi:10.1111/j.1745-9125.2009.00139.x

Udoka, C. O., & Ogege, S. (2012). Public debt and the crisis of development in Nigeria econometric Investigation. *Asian Journal of Finance and Accounting*, 4(2), 231–243. doi:10.5296/ajfa.v4i2.2028

United Nations. (2005). *The Millennium Development Goals Report*. New York: United Nations Publications.

Virginia, A. M. (2005). *Introduction to sociology of education*. Lagos: DMMM Publishers.

Wolfgang, M. E., Thornberry, T. P., & Figlio, R. M. (1987). *From Boy to Man, from Delinquency to Crime*. Chicago, IL: University of Chicago Press.

Development of Crime Sociology From Bureaucratic Iron Cage to Digital Determination

1

Muhammet Ali Köroğlu

Uşak University, Turkey

INTRODUCTION

As a necessity of being a social being, humans have lived as groups and in communities throughout their entire history. The collective life has required some values, norms, and rules. As normative qualifications for human behavior values, norms, and rules are based on social order and the continuity of social life. For a very long period of time, social institutions, such as religion, morality, and politics were determinants on the individual and social behavior of human beings. Legal systems were then created and the provision of the behaviors was determined in detail. It can be said that legal systems are based on the negative behaviors of people, namely their criminal behaviors. However, there have always been individuals who violate the rules and legal norms required by social life. In its most general form, behaviors that violate the rules can be expressed by the concept of crime. Although the legal response of any behavior varies according to societies, crime is a sociological phenomenon that exists in all societies. Thus, Emile Durkheim, who describes “crime” as an action deviating from social rules, also defines a certain amount of crime as “normal.” After the first sociology classics, all the theories that emerged in the study of crime can be evaluated in different categories, such as sociological, psychological, and biological (physical, mental character). All these theoretical approaches explain some aspects of reality related to classical criminal behavior. However, new approaches are needed to explain the crimes committed in today’s virtual world.

With the previous revolution of human civilization, people have experienced the freedom of time, space, and labor. This situation was criticized by Max Weber (2000) as being a bureaucratic iron cage. In the last 50 years of human civilization, most people who became acquainted with the Internet considered it a freedom, transparency, and participation in the process of knowledge creation. However, it was understood that the world of the Internet could be an area in which all of the criminal acts known in classical literature could be realized. Moreover, by getting rid of all the restrictive norms that exist in the social world, a field of discharge has emerged in which man can act with the “id” completely in the Freudian sense.

First of all, the distinction between public and private spheres has disappeared. Thus, the Internet has become a field for socialization, anonymization, and catharsis. This has turned the Internet world into a risky area for many crimes, from property and personal crimes to crimes of terror. For this reason, the legal systems have had to further develop and create new security measures. Thus, a new social control mechanism has been developed through the security of the Internet world and its actions. It is likely that humanity would also be sentenced to the digital panoptic cage from Max Weber’s bureaucratic iron cage (Weber, 2000).

DOI: 10.4018/978-1-5225-9715-5.ch015

BACKGROUND

Crime refers to a negative value of human behavior. The act of valuing human behavior is carried out by others. Man is the only living creature capable of producing ideas about himself and his environment, questioning the value of his behavior, and seeking out the ideal. The history of humanity is the history of the effort to achieve the best for human existence. The act of crime is a phenomenon that is always present as the dialectic of this humane effort. For this reason, as a necessity of being human and being social, virtuous behavior, as anti-crime behavior, covers the whole of human history.

Throughout history, all societies have sought to determine and evaluate the behavior of their members in order to protect themselves and their social systems. For the valuation of behaviors, social institutions were produced. Social institutions, such as political systems, the legal system, religion, and family, have provided limits and legitimacy in all areas of life in which the actions of the individual can be related, and this is still the case. Human behavior may be related to the individual himself, other human beings, the social and political system he lives in, the ecological system, and, if he believes in a particular religion, his God. For all these fields, all societies produce mechanisms that set values and limits to individual behavior. The crime phenomenon emerges as a deviation from the legitimacy standards set by these mechanisms. For this reason, all societies want to control the behavior of their members and gain the behavior habits that they accept as ideal.

It is possible to find this thought even in the works of intellectual personages of the ancient age. Aristotle and Plato viewed crime as the negative extremism of human emotions and actions. Justice was considered as the balance of feelings and actions. However, there are some acts, such as theft and murder, and these acts are considered harmful and criminal. For human actions in this regard, the balance situation is not sought. According to Ross (1993, p. 239) individuals can gain virtuous behaviors through the educational institution. The phenomenon of crime, although changing from society to society, is a phenomenon that is always present and discussed. This discussion also brings about a discussion of how to control human behavior. Throughout civilized human history, an internal control had been targeted through the religious institutions. In the same way, external control was attempted through political institutions. Most of the time, the political control mechanisms supported by the religious institutions worked together. Thus, the orders of God and the king have drawn the boundaries of legality and crime together. After the understanding of science created by the age of enlightenment, science began to put limits on human behavior.

Each individual plays the roles they have defined for themselves in the social life by occupying the designated status. The only area in which an individual can act freely and in his own capacity is the private sphere. In the modern period, it for humanity's social behavior to be controlled by institutions, such as work, school, hospitals, prisons, etc., has been criticized by many social scientists. While Karl Marx (2000) criticized the process of alienation and the loss of human creativity, Max Weber (2000) envisioned the boundaries of human actions to a bureaucratic iron cage. Weber (2000) defined the rational, soulless, and emotionless social world as a world whose magic has deteriorated. In the next process, the private sphere, which is the only area where human behavior is not identified, is now invaded by millions of eyes via the Internet. The phenomenon of crime, representing the dark side of human nature, reinvents itself with new communication possibilities and technologies.

Today, with the accessibility of the Internet a reality in the lives of most individuals, the act of crime undergoes a structural transformation with the redefinition of time and space. This structural transformation also transforms the control mechanisms relating to human behavior. The virtual world offers the

possibility of crime, as well as the possibility to monitor and control human actions that are likely to commit crimes. In the context of Internet and artificial intelligence opportunities, the psychosocial processes that enable the emergence of criminal behavior should be re-evaluated. In fact, starting from the definition of the concept of crime, criminal theories should be considered in relation to the new situation.

When the literature on crime phenomenon is examined, it is seen that crime is evaluated by the fields of sociology, psychology, biology and neurology. Since these areas address different aspects of human reality, their definition of crime also changes. Therefore, new perspectives on crime should be developed by reassessing the theoretical approaches of the related fields in the context of contemporary artificial intelligence and Internet technologies.

THEORETICAL APPROACHES ON CRIME

Crime is an act that is essentially committed in violation of a law, or by not performing the behavior required by law. The law is officially applied rules by a political authority. The elites, who generally possess state or state power, define crimes as actions that violate the norms and values strongly accepted by society (Zastrow, 2013, p. 406). The concept of crime is mostly evaluated together with the concept of aberration. Aberration refers to behaving differently from behaviors considered normal and correct in a society (Zencirkiran, 2016, p. 231). The concept of aberration in everyday language means deviating from an accepted path. In this respect, it expresses the behavior that is not appropriate to the expectations and norms of a particular group. Aberration can be rewarded, punished, or accepted, without reward or punishment (Göktuna Yaylacı, 2012, p. 181). In a society, no one completely violates the rules, and no one completely obeys the rules. In some cases, most people break some generally accepted codes of conduct (Giddens, 2000, pp. 182-183). However, each violation of the rules may not reveal the category of crime and punishment.

The Sociology Dictionary links the concept of crime with law and authority. “Crime, according to Marshall’s (1999, p. 702) definition is, “An action that exceeds the personal sphere, including the boundaries of public sphere, and violates the rules and laws that are prohibited, requiring intervention of penalties or sanctions or a public authority (state or local institution).” According to this definition made from a sociological perspective, the actions outside the borders of the legal order are considered crimes. Aberration is a concept close to crime, but refers to actions that do not include the evaluation of the judicial system. Aberrant behavior is punished by social control mechanisms, such as values and norms, until it reaches the legal system. Considering whether a behavior is applied sanction by the legal system or society, it is possible to decide which category will be evaluated as a crime or as an aberration (Dolu, 2013, p. 3). Accordingly, the legal system punishes criminal behavior and the social system punishes the behavior of aberration.

Whether they are legal crimes or social aberrations, undesirable behaviors that are subject to social and institutional intervention continue to exist in all societies. The oldest types of crimes in the memory of humanity, such as murder, theft, and sexual assault, have evolved into new forms by evolving in modern society. While deviant behavior in the human fiction of modernity was defined as irrational behavior requiring reformation, the technological possibilities provided by the Internet also provided new forms and avenues for criminals. Criminal behavior, which is a multidimensional subject, is widely evaluated in terms of predicting human behavior, changing and controlling human behavior, political power, and

physical health standards. Therefore, theories about crime and deviant behavior are developed by sociology, psychology and medical disciplines in the context of the human imagination of modernity. It is possible to talk about many theories, but it is important that these theories are re-interpreted in relationship to the Internet and artificial intelligence (AI). First of all, it is important to determine the place of crime and aberration in modern society's understanding of humanity and civilization.

Modern Society and Crime

In the world of social sciences there is a significant amount of literature on modernity. As a result of a significant effort, modernity is determined by scientific, cultural, political, and industrial revolutions (Jeanniere, 1993, p. 97). It is stated that concepts, such as progress, evolution, freedom, democracy, and equality, which are the basic ideas of modernity, are possible through the liberation of the human mind (Paz, 1993, p. 185). Basically, in these principles based on the idea of enlightenment, freedom is designed as a function of the mind. According to this, man can understand and re-establish the reality of humanity and society through the mind and science. The truth about man and society is universal because the human mind and science are universal. Therefore, it is essential to rebuild life according to the universal reasoning and scientific criteria (Şaylan, 1999, p. 134). Thus, human design, as a universal unitary subject, thinking and acting with a universal mind and science, is revealed. People with common behaviors who are away from tradition, superstitious beliefs, and sensuality, acting with the same mind all over the world are foreseen. The natural consequence of this can be a period of humanity in which crime, aberration, war, and destruction become history; the common man transformed into a superior man. However, today's realities do not coincide with society's expectations. Crime, aberration, and humane disasters have become more and more sophisticated in today's world than they were throughout all periods of history, and this is due to the availability of new technologies that have opened up more ways for people to communicate and socially interact, such as through social media channels on the Internet.

It is possible to see one of the most effective criticisms of determination and identification of human behavior in Weber's (2000) research. His concept of bureaucracy refers to the hierarchy and behavior patterns defined within the framework of rational action logic. Once a bureaucracy has been established, it does not mean that only one work is most rational and profitable. It becomes a social structure that cannot be eliminated. Bureaucracy becomes a means of transforming collective action into social action, which gains rational regularity. As a means for socializing power relations, a bureaucracy becomes the most important instrument of power for those who control this apparatus (Weber, 2000, p. 311).

Bureaucrats cannot control the system because they become part of it; they cannot prevent its functioning and cannot move flexibly. All this can be possible through the power at the top of the hierarchy. Here, then is a case of determining of human behavior in the finest detail. As a result, modern man is obliged to the boundaries of the iron cage of the bureaucracy supported by other social institutions such as education. Despite these limits, crime, corporate crimes, murder, and sexual offenses, remain in existence by changing form. The determination of human behavior totally by the owners of property is criticized by Karl Marx (2000, p. 27) as the alienation of man from himself, his nature, and his labor. In this critique, criminal behavior arises in the context of contradictions in the relations of production and property. Sociologists from the Marxist tradition regard crime as a consequence of capitalist class relations. According to them, all crimes, such as organized crime, murder, and theft, are determined by structural factors.

The human and order design of modernity, and the control mechanisms created accordingly, are criticized by many social scientists including Michael Foucault (2015) and Zygmunt Bauman (1997). Foucault, in his books titled, “Madness and Civilization” and the “The Birth of Biopolitics,” extensively describes how the modern period condemns the differences and confines the person (Foucault, 2015, pp. 7-715).

In the same way, Bauman (1997, pp. 30-32) attempts to understand modernity by the metaphor of a garden design. In this design, uncontrollable behavior is an unacceptable crime. In modernity, man has to be predictable, supervised, and controlled. Throughout human history there has never been full equality between the crime and the control mechanism. For the first time, through modernity, it is seen that surveillance and controlling mechanisms are ineffective against crime. Nevertheless, all known crimes exist by making use of the same technologies and control opportunities.

Emile Durkheim (1992, 2006), one of the first sociologists of modernity, describes crime as pathology. This is a biological concept. Crime and aberration is a social phenomenon considered normal in the sociology of Durkheim. While examining the crime, Durkheim examines the concept of punishment as a requirement of his sociological method. Crime is the act that leads to a special reaction called punishment against the offender. While there are some universal offenses, such as murder and theft, these crimes are few. However, in all societies there are many criminal behaviors that require punishment. This is about the essence of the concept of crime. According to Durkheim, the essence of the concept of crime represents a rebellion against social conscience. Society imposes the punishments necessary to maintain its integrity. The types of penalties vary according to the types of solidarity of societies. As crime and aberration are directly committed against the collective soul in mechanically solidarity societies, a punisher law is essential. On the other hand, because of the division of labor in organic solidarity societies, punishment is determined by the principle of restorative law (Durkheim, 2006, pp. 99-216).

Additionally, Durkheim states that social control is lost and anomalies occur during periods when social rules are obscured (Durkheim, 1992, pp. 245-264). Anomy, or social instability, refers to the situation in which social norms lose the power to regulate and discipline human actions. In such a situation where norms are absent or contradictory, the individual loses the measure of their behaviors. Thus, anomy becomes the cause of behaviors deviating from norms (Dönmezer, 1999, p. 236). This is due to rapid social changes. Individual norms do not work. The individual cannot know new norms. So, there are aberrations at the social level. The modern period foresees a social structure that raises risks and dangers against the sense of security, which is one of the most basic needs of man. The working principle that destroys creativity, threats that cause fear, such as the threat of nuclear war or totalitarianism, are not as not real to modern human beings, as it was to segments of humanity in past periods (Giddens, 1998, p. 16-19).

Modern human behavior takes place in the social world of such a tension, and a crime is formed. The most satisfying approach to the nature of criminal behavior has to be sociological because the nature of the crime depends on social relations and social institutions. Sociology emphasizes the reciprocal connections between adaptation and aberration in different social contexts about the phenomenon of crime (Giddens, 2000, p. 186). The theoretical approaches in the sociological context, such as labeling, learning, differential unity, and anomie, address the context of relationships, acceptances, incentives, and limitations in which human behavior emerges. Human attitudes, emotions, thoughts, and actions are shaped according to the values of his or her society and human understanding. No human being is absolutely well programmed and does not have to behave well. Likewise, no human being is absolutely bad

and is not programmed to commit a crime. Man, as the founder of civilization and the bearer of virtues, is also, as Thomas Hobbes (2019) predicted, selfish, egoistical, manipulative, and a merciless creature in pursuit of power. What determines this difference according to sociology is the social environment in which the individual develops.

Digital Identity and the Modern Actor

Identity, as a sociological concept, is the name of a process that occurs within the framework of the individual's relationship to society. In one aspect, it ties the individual to the society in which he or she lives and differentiates him/her from others. The individual's attitude towards social expectations constitutes his/her identity. The individual becomes a member of society through the process of acquiring an identity, interprets social expectations according to his/her own ideas and values. Thus, the individual's interaction with his or her society acts as an identity formation process, and this process lasts for a lifetime. Each individual creates common behaviors, values, expectations, and norms, as well as differences.

The concept of identity in the modern era is formed within the framework of the concepts of public sphere, state, citizenship, and autonomous actor. The relationship between the individual and the state is established by citizenship laws, and a sense of belonging is created (Marshall & Bottomore, 2000, pp. 36-50). The public sphere emerges as a discursive field where the individual, as a rational actor, expresses his/her own demands and expectations. The real determinant of identity is the public sphere, because identity is manifested as a concept shaped by modernity. The identity is given to the actor and it becomes a part of the public sphere. The fact that the actor can participate in the public sphere without being declared guilty or banned obliged to acceptance of this identity which is presented by modernity. This identity, defined by modernity, depends on acting as someone with the principles of universal rationality. Thus, reason, law, science, morality, and the actor, become universal with this principles. As a result, the modern public sphere pushes the specificities, localness, and differences of the actor, whom it considers irrationally, into a private sphere. The public sphere turns into the field of cultural and political power of modernity (Karadağ, 2006, p. 55).

In today's modern era, the sociological context of the concept of crime develops on the basis of individuals and groups excluded from the public sphere. When the groups excluded from the public sphere are examined closely, ethnic groups, religious groups, women, ghetto inhabitants, and people living in poverty, come to the fore. Ethnic, religious, and cultural exclusion forms the basis of terror, drug trafficking, human trafficking, murder, ransom, and all kinds of political crime. Poverty and demographic intensity in the ghettos provide a broad culture of crime, ranging from theft to sexual crimes. On the other hand, the criminal behavior of individuals and groups who express themselves in the public sphere is more qualified and more sophisticated. Corporate crimes, tax evasion, money laundering, and crimes against human dignity are committed according to the rules of the universal system. Then, with the development and socialization of mass media, the concept of a homogeneous public sphere changes in structure and function. Mass media becomes an economic value and begins to determine public opinion according to private interests (Habermas, 1997, pp. 309-328). The elements belonging to the whole private sphere and different identities begin to involve into the public sphere, which is the special design of modernity. The public sphere is attacked by the private sphere, and the distinction between the public and the private spheres is almost lost. While mass media is accelerating this process, the Internet is the largest transforming power.

The Internet is a universal public sphere that connects the whole world, and it is very difficult to control (Bacık, 2005, p. 15). The internet allows all identity groups to be present in the public sphere. Due to the Internet, the expectations of the actors who have been established in the modern world, transform. At the same time, the nature of the actors and the crimes transform. Crime is committed not by the identities included from the marginal neighborhoods or excluded from public spheres, but by actors having higher social status and advanced education. The crime becomes independent of time and space, and moves up the social ladder (e.g. white collar crimes). Certainly, traditional crimes such as murder, extortion, and theft remain the same, however, major crimes are being committed through Internet opportunities. Traditional crimes that can be committed using the Internet include crimes such as threats, blackmail, attacks on bank accounts and credit cards, seizure of digital objects, sexual offenses, pornography, terrorist offenses, terrorist propaganda, and infiltration into security systems can be more easily committed than by using traditional criminal methods.

The world of virtual relations supplied by the Internet provides a space in which individuals communicate with their social identities outside the limits of all social norms and values. The person communicating through the Internet may disclose his/her gender, age, ethnic characteristics, and social status as unlike his/her true characteristics and life. Anyone can become a personality that he/she wants to be, or wants to see, but never feels comfortable being in the real social world. This is the process of disidentification by contrast, with the identities attributed to the individual through the modernity.

It is impossible to predict the dimensions of the disidentification process. An individual can watch a child rape with great pleasure in the confines of his room via the dark Internet world on a nightly live broadcast, and the next day, that same individual can talk at a conference on children's rights, as a requirement of his esteemed status. The structural personality theory proposed by Sigmund Freud (as cited in Ceyhan, 2013) might be illustrative in explaining the infinity of crimes related to identification and disidentification.

Freud believed that unconscious forces and internal conflicts played a decisive role in determining the individual personality. According to Freud, the personality structure consists of three structures: id, ego and super ego. These structures are supported by the libido, as the psychic energy. These structures form at different stages of an individual's development and are in mutual interaction (as cited in Ceyhan, 2013, p. 94). One of the most fundamental components of the personality structure, id, is genetic spiritual energy. The id includes biological, instinctive behavior patterns such as eating, drinking, sexuality, and aggression. The id acts in the sense of pleasure and satisfaction for instincts. The id's effort of satisfaction does not accept time, space, or social boundaries (as cited in Ceyhan, 2013, p. 94). The id constitutes the most primitive dimension of the human self and does not accept any excuse for the pleasures that it demands. In contrast, the ego is the center of the human personality and acts with the principle of realism. Through contact with the real world, the ego controls consciousness. It determines rationally how to be satisfied in the real world by controlling the demands of the self. The super ego is the moral and social aspect of the human self (as cited in Ceyhan, 2013, p. 94). While the ego forms the rational dimension of the human self, the super ego forms the moral and social aspects of the self. Criminal activity derives from the deterioration of balance between these personality elements. For a balanced personality, a demand requested by the id, is judged through the ego, and met, if it is suitable to the super ego. However, if this balance deteriorates, the demands of the individual's primitive aspects try to become satisfied in the social world. Thus, crimes come into existence in the real world.

The process of disidentification in the Internet world also functions with the same mechanism. All demands from the id are transferred to the virtual world uncensored. For the most primitive demands that can never be imagined in the social world, the virtual world becomes a field of discharge. There is no mechanism to run the super ego. The ego confuses reality and virtuality, thus, primitiveness and savagery can find a place in the virtual world more easily than ever before in human history.

The id, as the primitive component of the human self, cannot be limited and it is not possible to limit the crimes committed in the Internet world, especially on the dark Internet. Rather than a traditional armed bank robbery, it is very comfortable to rob a bank in London by sitting in a remote town in Asia and transferring money from one account to ten accounts. Moreover, national boundaries and legal systems do not apply to the digital world. The largest value of this unlimited world, established with Internet networks, is data. Those who control the data, also control the lives of others. All kinds of digital operations, GPS devices, mobile phones, computers, credit card transactions; basically, all actions in daily life, leave a lot of data behind them. It is possible for malicious people to control the life of an ordinary person by accessing and using the person's personal data.

Thus, the virtual world turns into an area where many offenses can be committed very easily, such as sexual harassment, identity, data and bank theft, child abuse and pornography, murder and drug transfer, blackmail over photos that could discredit individuals. Moreover, centralized control over the Internet is impossible, because the Internet is a shared area. It does not have one owner. It is also technically very difficult and costly. For this reason, it is not possible for national auditing and international agencies to follow-up on crimes committed via the Internet (Taşkın, 2008, p. 16). The crimes of the former world are becoming a part of more people's lives today due to the new technologies. The former criminal organizations intervened more categorically with human life through gigantic data (Goodman, 2016, pp. 125-141). The biggest victim of this situation was the individual. The individual is alone and vulnerable against the criminal world. Global corporations and national strategic data units spend millions of dollars developing new security measures. However, the national legal processes for the individual is handled very slowly and the individual often becomes a victim in this process. For this reason, it is possible to say that the biggest need of the digital world is the need for security, which Abraham Maslow, (1943) gives place to as the first rank, according to human necessities.

The problems here are the globalization of the interaction over the Internet, the monitoring and control of all kinds of data belonging to the users from all over the world, and the lack of defense power of the individual. When control systems, such as Promis, Echelon, etc., and global surveillance systems are added to this situation, the control over people reaches the most advanced level in history (Dolgun, 2005, pp. 186-187). With such programs, the individual can be monitored by the intelligence services in real time and in space with their voices by being analyzed by the use of artificial intelligence or by their images being monitored by any security camera. There is no place left for the individual to hide from being traced. Moreover, this can be done not only by national security services, but also by any digital tool used by the individual, by economic national and international companies, or by criminal actors. Thus, the Internet becomes a tool of power. In the virtual world, the individual can be controlled and determined by the reason of the traces left behind him/her. As a result, the individual is being promoted from Weber's (2000) bureaucratic iron cage to a transparent, digital glass cage.

FUTURE RESEARCH DIRECTIONS

1

As long as the primitive dimension of the human self exists, the crime phenomenon will continue to exist in the same way, but it will change its forms. Often, crime actors are quick to learn new technologies. If the managers of the great observer and the powers of the big data perceive threats to their security, no individual has any place to hide. But criminals who target ordinary individuals and institutions in daily life will always continue to exist and commit crimes. Smart objects will be open to the control the malicious actions of people as long as they are connected to the Internet.

In the future, the control of everyday life can be completely abolished through the use of artificial intelligence that is still in development. Artificial intelligence is an advanced tool design that modeled the human mind (Aydın, 2013, p. 13). Artificial intelligence is a project that moves towards artificial person design. It can become similar to a human being who can perceive the environment as a person, analyze large amounts of data in the Internet database it is connected to, draw conclusions, and take action depending on this analysis. As such, artificial intelligence may become the security and military personnel of the future. AI can eliminate human error. For example, a toilet, equipped with artificial intelligence, can provide information about the health status of the individual each morning by performing a urine analysis using the AI technology. There are many predictions about the humane and useful aspects of artificial intelligence.

However, artificial intelligence performing analysis and synthesis just as human beings cannot lead to good results. Through the Internet, all artificial intelligences can communicate with one another, gain autonomous characters, renew themselves, and produce norms for human beings, and then become a threat to human civilization. Today's artificial intelligence projects, however, are far from coming to this stage. From this perspective, the project of artificial intelligence is very similar to the thought of a modern, universal, rational actor designed by the science mentality and based on enlightenment. Just as the modern actor, designed as a superior man, artificial intelligence is also designed as superior to a human. A machine that can renew itself and produce thought and action can enslave humanity. In such a world, the definition of crime may vary according to the implication of superior intelligence. However, a world in the control of such advanced artificial intelligence does not seem very possible. Artificial intelligence can analyze the data in a frame determined by humans, make comparisons and make decisions (Canan & Acungil, 2018, p. 172). However, even in situations where people cannot make comparisons, they can establish emotions, values, belief connections, and produce meaning. Upon a man's look to a woman, he can write a love story and makes sense out of death and life. Human relations create social institutions. Human life is holistic. Artificial intelligence analyzes instant data and decides according to the highest probability. The highest probability in the human world may not always be the best possibility. All of these technical developments may further colonize the human life and destroy human creativity.

CONCLUSION

Crime is as old as human history. All societies have produced values, norms, and legal systems to protect their social order, carry themselves into the future, and keep their social life sustainable. They have maintained social cohesion by controlling the behaviors of community members through these systems. Likewise, they have imposed punishments for behaviors that are non-compliant with the values, the

norms, and the established legal system. Institutions, such as religion, law, and values system produced in the context of social relations, have created legitimacy and border lines for human behavior. While values for human behavior from society to society have changed, some crimes are universally accepted as crimes. Crimes, such as murder, theft, and rape, are in this category.

The essence of criminal behavior and the mechanisms by which these behaviors emerge have been discussed in detail. The sociological approaches that have emerged within the framework of these discussions have addressed crime in the context of an individual's relationship to society. Some sociological theories have claimed that crime is learned in the process of socialization; some have claimed that criminal behavior has been internalized by labeling. On the other hand, some biological and medical theories have attempted to explain crime as a genetic and anatomical dysfunction. Psychological theories have tried to explain crime through psychoanalytic and neurological processes.

Even though the phenomenon of crime does not place in the human design of the modern era, it has always existed. Crime continues to exist as a dark dimension of the human self, by changing form in the era of the Internet and artificial intelligence. It will most likely continue to exist in the future. Whatever the level of human development and civilization, the basic crimes are the same. Criminal acts such as theft, murder, rape, and harassment have only changed dimensions. There are no differences between the robbing of a bank through the Internet and the robbing of a bank by physically breaking into a bank. In terms of the definition of the crimes, both are theft. Only the act of virtual crime has become independent of time and space.

The emergence of the Internet and artificial intelligence technologies into human life creates new opportunities for people with malicious intent in terms of crime, leaving the individual more isolated and vulnerable. In this respect, today's societies are societies where social trust is very low and the risks are very high. As long as human beings exist, there will be crimes that represent human egoism and greed, as well as human error.

REFERENCES

- Aydın, A. O. (2013). *Yapay Zekâ: Bütünleşik Biliş Doğru*. İstanbul: İstanbul Gelişim Üniversitesi Yayınları.
- Bacık, G. (2005). Kamusal Alan Tanımı Üzerine Bir Tartışma. In A. Erol (Ed.), *Sivil Bir Kamusal Alan* (pp. 9–17). İstanbul: Kaknüs Yayınevi.
- Bauman, Z. (1997). *Modernite ve Holocaust*. İstanbul: Sarmal Yayınevi.
- Canan, S., & Acungil, M. (2018). *Dijital Gelecekte İnsan Kalmak*. İstanbul: Tuti Kitap.
- Ceyhan, E. (2013). Kişilik Gelişimi. In G. Can (Ed.), *Eğitim Psikolojisi* (pp. 82–112). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.
- Dolgun, U. (2005). *Enformasyon Toplumundan Gözetim Topluma*. Ankara: Ekin Kitabevi.
- Dolu, O. (2013). Suç ve Sapma Teorileri. In A. Geleri (Ed.), *Suç Sosyolojisi* (pp. 3–24). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.
- Dönmezer, S. (1999). *Toplumbilim*. İstanbul: Beta Yayınları.

- Durkheim, E. (1992). *İntihar*. Ankara: İmge Kitabevi.
- Durkheim, E. (2006). *Toplumsal İşbölümü*. İstanbul: Cem Yayınevi.
- Foucault, M. (2015). *Deliliğin Tarihi*. İstanbul: İmge Kitabevi.
- Giddens, A. (1998). *Modernliğin Sonuçları*. İstanbul: Ayrıntı Yayınevi.
- Giddens, A. (2000). *Sosyoloji*. Ankara: Ayraç Yayınları.
- Göktuna Yaylacı, F. (2012). Hukuk, Suç ve Toplum. In N. Suğur (Ed.), *Sosyolojiye Giriş* (pp. 167–202). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.
- Goodman, M. (2016). *Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü*. İstanbul: Timaş Yayınları.
- Habermas, J. (1997). *Kamusal Alanın Yapısal Dönüşümü*. İstanbul: İletişim Yayınları.
- Hobbs, T. (2019). *Leviathan*. İstanbul: Yapı Kredi Yayınları.
- Jeanniere, A. (1993). Modernite Nedir? In M. Küçük (Ed.), *Modernite versus Postmodernite* (pp. 95–132). Ankara: Vadi Yayınları.
- Karadağ, A. (2006). Kamusal Alan Modelleri Çoğulcu Perspektiften Bir Değerlendirme. In A. Karadağ (Ed.), *Kamusal Alan ve Türkiye* (pp. 42–74). Ankara: Asil Yayınları.
- Marshall, T. H. (1999). *Sosyoloji Sözlüğü*. Ankara: Bilim ve Sanat Yayınları.
- Marshall, T. H., & Bottomore, T. (2000). *Yurttaşlık ve Toplumsal Sınıflar*. Ankara: Gündoğan Yayınları.
- Marx, K. (2000). *Yabancılaşma*. Ankara: Sol Yayınları.
- Maslow, A. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370–396. doi:10.1037/h0054346
- Paz, O. (1993). Şiir ve Modernite. In M. Küçük (Ed.), *Modernite versus Postmodernite* (pp. 184–206). Ankara: Vadi Yayınları.
- Ross, W. D. (1993). *Aristoteles*. İzmir: Ege Üniversitesi Yayınları.
- Şaylan, G. (1999). *Postmodernizm*. Ankara: İmge Yayınevi.
- Taşkın, Ş. C. (2008). *Bilişim Suçları*. İstanbul: Beta Yayınevi.
- Weber, M. (2000). *Sosyoloji Yazıları*. İstanbul: İletişim Yayınları.
- Zastrow, C. (2013). *Sosyal Hizmete Giriş*. Ankara: Nika Yayınevi.
- Zencirkiran, M. (2016). *Sosyoloji*. Bursa: Dora Yayınları.

ADDITIONAL READING

- Aydın, İ. H., & Değirmenci, H. (2018). *Yapay Zekâ*. İstanbul: Girdap Yayınları.
- Bauman, Z., & Lyon, D. (2013). *Akışkan Gözetim*. İstanbul: Ayrıntı Yayınları.

- Berger, J. (2018). *Görme Biçimleri*. İstanbul: Metis Yayınları.
- Biermann, W., & Klönne, A. (2007). *Kapitalizmin Suç Tarihi*. İstanbul: Phoenix Yayınevi.
- Fromm, E. (1996). *Çağdaş Toplumların Geleceği*. Ankara: Arıtan Yayınevi.
- Gençtan, E. (2014). *Psikanaliz ve Sonrası*. İstanbul: Metis Yayınları.
- Lyon, D. (2013). *Gözetim Çalışmaları*. İstanbul: Kalkedon Yayınları.
- Norvig, P., & Russell, S. J. (1994). *Artificial intelligence: A modern approach*. New Jersey: Prentice Hall.

KEY TERMS AND DEFINITIONS

Artificial Intelligence (AI): A machine that can make decisions, produced by modeling human intelligence.

Digital Age: The period in which smart machines are determinative in social life.

Digital Cage: Refers to an opinion that every moment of the lives of individuals is under surveillance in the digital age.

Disidentification: The disappearance of an individuals' real social identifications in the digital world.

Public Sphere: The area of political and cultural discourse of the modern actor.

Social Aberration: Diversion from common social values and norms.

Sociology of Crime: A science discipline that examines the phenomenon of crime through a sociological approach in its historical process.

Section 2

Cyberwarfare, Cybersecurity, Spyware, and Regulatory Policies and Solutions

The Globalization of Hybrid Warfare and the Need for Plausible Deniability

Benedict E. DeDominicis

 <https://orcid.org/0000-0001-7743-717X>

Catholic University of Korea, South Korea

INTRODUCTION

This chapter analyzes the utilization of social media as part of hybrid warfare's efforts to undermine state security through covert means that can be illegal or criminal. It begins by highlighting the postwar globalization context that encouraged indirect and covert competitive intervention by nuclear powers within the internal politics of target polities. The post-1945 nuclear environment ended the viable application of deadly force as a purposeful policy option for great powers intentionally to select in order to attain their goals regarding each other. They battle indirectly through competitive interference within the political systems of third actors in addition to targeting not only each other, but also their own national public opinion. The aim of this competitive interference is to enable their respective local political clients at the expense of the perceived local clients of the other intervening competitor. The growth of mass public participation intensified nationalist self-determination political sensitivities. It increased local opposition and raised the political costs of overt external interference. Postwar global human rights norms developed to include national self-determination for all. Covert intervention abroad became politically preferable domestically as well to avoid negative domestic political reactions to perceived imperialism. Covert intervention in all forms decreases political resistance and costs to the intervenor. This chapter highlights how the nature of social media content distribution makes propaganda and disinformation distribution very extensive at relatively very low cost. These trends and advantages furthered the stress on covert intervention and the formation of national security bureaucracies for engaging in it. Social media propaganda operations are branded as disinformation because their source is purposefully disguised. Russian state agency Internet-based covert intervention via social media in the 2016 US national elections demonstrated that the US is part of the politically globalizing world that it helped create after 1945. The policy response to these challenges is likely to include strengthening further the intelligence/counterintelligence capabilities of the national security state.

BACKGROUND

Adamson (2005) argues that due to American-led postwar economic and political globalization, the differentiation between external and internal security threats is increasingly blurred. “[N]ew security strategies of global policing [and] surveillance [...] that emerge in response to this new environment will need to be accompanied by a set of new political strategies” (p. 44). Soviet-American global competition for political influence in the nuclear setting provided the template for what is today labelled hybrid/cyber warfare including security policy responses to it. “The covert aspect of information and propaganda dissemination ... has been of exceptional importance during the Soviet-American cold war” [*sic*] (Cottam

DOI: 10.4018/978-1-5225-9715-5.ch016

& Gallucci, 1978, p. 32). This external intervention, when observed by mobilized local political actors, would more likely be seen in effect as an intolerable violation of national sovereignty. This interference would contribute to intensifying domestic polarization within the target polity. The exacerbation of the perceived threat from the other would thus appear to vindicate the intervention by their respective external patrons in the eyes of each local client. Disinformation as a component of what is frequently called “hybrid warfare” encourages mobilization to meet the perceived threat (Isikoff & Corn, 2018, p. 44). The local competitor and its external backer depict this resistance-themed disinformation against the alleged threat to national sovereignty as in essence local. The external encouragement and support for one side or the other is purposefully disguised, if not concealed (Voss, 2016, p. 40). The multiple facets of elaborate disinformation campaigns may or may not be illegal. E.g. Russian hacking and theft of more than 150,000 emails from personal or Democratic National Committee linked email addresses was illegal. The intensely competitive for-profit US news media’s utilization of these surreptitiously provided emails via Wikileaks, weakening the Hillary Clinton 2016 presidential campaign as Moscow intended, was not. The complexity of the context intentionally obscures the external intervention in the view of local political actors.

The extent to which this resistance to outside intervention within internal politics may be plausibly portrayed as essentially local was limited. Completely masking external involvement engaging many individuals is not feasible. Aside from the exploitation of new Internet media and communication infrastructure technologies, Washington and Moscow displayed this covert policy behavior historically long before 2016 (Renz, 2016, Ransom, 1977). Target polities included domestic public opinion in addition to foreign publics (Wilford, 2017). Today, so-called hybrid warfare combines national security organizational resource deployments along with exploiting Internet-based technologies to affect the target polity’s power capabilities (Cottam & Gallucci, 1978). The latter include covert psychological social media-oriented public opinion campaigns and damaging Internet-based infrastructure hacking attacks to achieve national security and foreign policy objectives.

Self-determination concomitantly has developed into a human right, although one controversially delineated (Cassese, 2005, pp. 16, 39, 63, 75, 84, 207). Foreign meddling in a targeted polity’s internal political concerns is likely to be condemned by at least some attentive constituencies in the target polity as a desecration of this national community birthright. Determining whether or not it is actually illegal and criminal prevention and punishment is enforceable depends upon the specific legal and political conditions within the target polity. Social media and the Internet in general have expedited this intervention. They have also provided greater opportunities to obfuscate the architect of this interference.

Concurrently, one’s own unofficial collaboration with foreign actors is likely to be self-servingly viewed as not being seditious. The alliance may be formal, i.e. overtly or covertly with intent to receive funds and other material support from a foreign actor. The association may be implicit, such as benefiting from foreign-subsidized social media disinformation operations which were not directly entreated by the local client, but the latter is aware of the intervention. Since the outlay of support was not in the form of a direct disbursement to the local client or other direct donation, it may be more easily categorized as inconsequential. Certain Western political figures and their constituencies view Putin’s regime in Russia as a stronghold for traditional, so-called Christian, conservative family and national values. Post-Soviet era informal collaboration by American partisan competitors with Putin’s regime is therefore less prone to be regarded as potentially treasonous. Rather, it is another alternative resource to oppose the potentially treasonous assimilationist cosmopolitanism that so-called globalist values and their transnational and local collaborator constituencies advocate. According to this conservative populist nationalist worldview, these cosmopolitans are allegedly a threat to the nation’s sovereignty and thus ultimately to the nation’s very existence.

FOCUS OF THE ARTICLE

The Globalization of Hybrid Warfare

Cassese defines globalization as the “close intertwining” between most components of national structures and of the external, international community. The latter includes “individuals, groups, associations, State-like entities, multinational corporations, trans-national organizations, multinational financial structures, media networks, etc.” [*sic*] i.e. any external actor that is not a state (2005, p. 5). In international relations, states nevertheless remain the most important legal “person” by far despite globalization (Shaw, 2014, p. 143). In the highly decentralized and primitive international legal system, states not only are the subjects of international law. They also each individually make international law through treaty agreements and customary behavior. They interpret its obligations, as well as enforce these obligations on each other (Cassese, 2005, p. 6).

Proving intent to participate intentionally in a criminal conspiracy or collusion is necessary for a felony conviction on a charge of distributing illegally obtained classified or proprietary information. “Among the great advantages cyberspace offers to criminals are anonymity and the ability to allow otherwise unassociated individuals in different parts of the world to network on a transactional basis” (United Nations Office on Drugs and Crime, 2010, pp. 203-4.) Consequently, “organizations as diverse as the ISIS and the Zeta Cartel are using cyberspace to shape opinion and elicit respect, fear and terror” (Muggah, 2015, para. 3).

Intermediaries between Julian Assange, Wikileaks’ founder, and Russian intelligence agencies providing hacked Democratic National Committee (DNC) emails facilitates legally plausible deniability regarding Assange’s intent in publishing them (Cormac & Aldrich, 2018). Gaughan claims that the 1970’s-era US Federal Election Campaign Act (FECA) is outdated; the evidence is not clear that the Trump campaign’s Russian support was illegal under FECA (2018, 104). Trump in mid-2018 enjoyed exceptionally stable and high approval survey ratings among Republican party self-identifiers at 88%, while 7% of Democrats rated his performance positively (Dunn, 2018). Among Trump partisans, treason did not occur; indeed, their rejection of the claim reflects their disdain for Trump opponents who attempt to make it an issue to weaken Trump domestically. Republican party self-identifiers disincline to share the perception of post-Soviet, anti-globalist Russian foreign policy behavior and capability as being directly threatening to the US. Benefitting politically from Russian involvement within the US polity does not establish treason. Profiting from Russian influence does not validate the effort to nullify the 2016 US presidential election outcome and the subsequent US foreign and domestic policy process outcomes that derive from it.

Aggregation and analysis of social media user data permits microtargeting to concentrate advertisements towards specific audiences to strengthen emotional antagonism regarding other groups within the state. Intensification of polarization by Russian covert state agents via the Internet in the midst of some constituencies fearing globalization extends even to current controversies such as the effect of vaccines (Broniatowski et al., 2018).

Undermining state’s power capability can comprise undermining governmental and, more deeply, regime stability by aggravating the intensity of political polarization between constituencies within the polity.

According to a top-secret NSA [US National Security Agency (BD)] report issued more than a year after the U.S. [2016 (BD)] election, the [Russian government's covertly-sponsored (BD)] Internet Research Agency conducted information warfare along several fronts. One was referred to as “govstrana”—which the NSA translated as “crap country”—and referred to attacks meant to damage a nation’s reputation and sap its citizens’ confidence. This effort involved the creation of two types of trolls (the term for online provocateurs), one focused on influencing public opinion by amassing loyal followings, and another that used teams of four or five people to churn out a mass volume of posts to overwhelm any competition from those posting contrary opinions (Miller, 2018, p. 39).

Howard, Ganesh, Liotsu, Kelly and Francois (2018) report that the IRA’s distributions reached tens of millions of users in the US between 2013 and 2018. More than thirty million users shared the IRA’s Facebook and Instagram posts amidst liking, reacting and commenting on them. The IRA’s “activities began on Twitter in 2013 but quickly evolved into a multi-platform strategy involving Facebook, Instagram, and YouTube amongst other platforms.” They note that the most far reaching IRA social media activity was not in the form of paid advertising, but rather through social media user/consumer distribution of IRA posts, i.e. organic posting (p. 3).

Increasing the intensity of public political polarization can help undermine the national mobilization capability available to state authorities to extract and direct societal resources for achieving policy goals (Cottam & Gallucci, 1978, pp. 10-22). Rising political dysfunctionality can likewise undercut the international attraction of the ideology that a specific government asserts it represents as a function of its international influence capability (Ibid.).

The tactical goal in covert disinformation operations is to intensify existing polarizations within the target polity. Miller reports that the Russian military journal, *Military Industrial Courier*, published a speech by General Valery Gerasimov, chief of staff of Russia’s armed forces, in 2013. Gerasimov outlined the harnessing cyberattack capabilities. “[T]he role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons” (quoted in Miller, 2018, p. 28). The function of social media in enabling what developed into the Arab Spring seemingly demonstrated the practicality of social media for attaining preferred political developments in targeted state actors. “Frontal engagements” by military forces are to become “a thing of the past” (Isikoff & Corn, 2018, p. 44). The St. Petersburg state sponsored covert cyber operations unit, the Internet Research Agency, demonstrated the usefulness of cyber operations as a component of hybrid warfare tactic during the 2016 US presidential campaign. Occupying a four-story building, it produced content that via Facebook reached an estimated 126 million Americans during the 2016 US presidential campaign (Miller, 2018, pp. 36, 181). The degree of American cultural discourse awareness and sophistication in the Agency’s ongoing “Project Lakhta” American polarization promotion disinformation campaign has increased (Ohlin, 2018, p. 22). US government agencies have initiated counter-measures, e.g. the US Justice Department in September 2018 revised policy regarding “Disclosure of Foreign Influence Operations” (Ibid., p. 18).

Social Media and Societal Polarization

Social media internationally has exacerbated polarization surrounding persistent racial, ethnic, sectarian and cultural fault lines because of the features of the social media for-profit business model. Social media account owners choose to receive content from specific distribution lists for particular types of

content, including content that represents itself as news reporting and analysis. Social media distribution relies on algorithmic methods to select and direct content irrespective of truthfulness to designated account owners. Facebook management decided prior to November 2016 to end human oversight of content feeds to users' accounts in order to avoid the appearance of subjective partisan bias to potential advertisers (Miller, 2018, pp. 183-91). These computer software algorithms route posted content according to account holder interest as extrapolated from their collective earlier content viewing choices, likes/dislikes, friends, and other inputs. A consequence has been the magnification of the so-called echo chamber outcome on citizen-consumer perceptions and attitudes that associate with stereotyping (DiFonzo et al., 2014).

During the Reagan administration, the US Federal Communications Commission encouraged this trend in 1987 by abandoning the Fairness Doctrine, adopted in 1949 by the Federal Communications Commission. The Fairness Doctrine required "a reasonably balanced presentation" of alternative political viewpoints, building on the 1927 Radio Act (Lepore, 2018, para. 7). Enforcement was rare (Clogston, 2016, pp. 377-78). The highly-competitive for-profit news media business produces items for consumption that interpret events in accordance with their respective editorial ideological inclinations. The modal citizen-consumer tends to favor news media consumption selections which conform with their existing political perceptions and predispositions. Incongruous information reports and analyses which generate disagreeable emotional reactions due to conflict with these intensely held beliefs and attitudes can much more easily be dismissed. The upshot is to strengthen pre-existing citizen-consumer political assumptions and viewpoints on the range of topics. The vastly larger variety of news sources has greatly increased the ease of self-validation of political self-identity for the media citizen-consumer through finding confirmation in news reporting. They can find seeming endorsement for their pre-existing, strongly held political views from intensely competitive for-profit news media product purveyors. The latter forcefully profess to be current events authorities in their marketing campaigns. They thereby support the citizen-consumer's self-validation while embracing membership in a legitimated community of more or less self-conscious fellow ideologues. Their outlooks incorporate shared implicit and explicit elements of favored worldviews regarding political cause and effect. These worldviews incorporate classification of malign and benign political players and their real or conspiratorially imagined influences. Intense emotional affect associates with stereotypical image formation (Cottam & Cottam, 2001, pp. 99-105). Actors more inclined to nationalistic behavior are more prone to stereotyping and emotional affect (Ibid., pp. 105-21).

Ideological framing of news reports tends to steer ultimately to explicit and implicit inferences regarding consequences for the well-being of the nation of these reported current events (Horton & Brown, 2018, p. 3). The conceptualization and definition of the welfare and even the survival of the nation are defined according to the respective worldview, i.e. editorial angle. Emotional affect among the market share/public audience/citizenry constituency is thus expected to be stimulated. It must be roused; emotional stimulus and satisfaction motivates consumption and citizen-consumer loyalty while contending for subscription and advertising income. The objectivity façade in news reportage must be upheld and homage paid to it as part of marketing for all news items to be propagated for consumption as news reports on current events. Maintaining this citizen-consumer loyalty in a fragmented, diverse collection of ideological niche markets has become a business success imperative. Serving, even pandering to these niche market demands to maintain market share tends to intensify and reinforce these preexisting viewpoints.

This competitive for-profit systemic logic for maintaining media-consumer/citizen loyalty tends to encourage the stereotyping of non-conforming views as not only flawed, but morally reprehensible. Reinforcing political in-group predispositions concurrently intensifies demarcation from out-groups

(Bruchmann, Koopman-Holm & Sherer, 2018). The news media functions figuratively both as an echo chamber for the citizen/media-consumer and also as an amplifier. A positive portrayal of the news media characterizes it as a collection of institutions where the citizen/media-consumer may subject their presumptions to examination via exposure to additional evidence. This ideal view perhaps always has been a positive stereotype. A conventional metaphor portrayed the news media as the “watchdog of democracy” (Orzeata, 2016, p. 135). Another trope depicts the news media as the conduit for the “marketplace of ideas” (Asenas & Hubble, 2018, p. 38). Yet, incongruous information was more difficult to evade or reject in the postwar era under the Fairness Doctrine and with television news restricted to three national networks.

The echo chamber effect is a term that highlights this source of political polarization along with the emergence of the Internet-based social media platform for media product distribution (Matakos, Terzi & Tsaparas, 2017). The growth of Internet social media has magnified and mobilized constituencies around these polarization cleavages, at times with violent, tragic results. E.g., a Sri Lankan militant in 2018 utilized Facebook to disseminate hatred and paranoia leading to an anti-Muslim riot killing one person and making many more homeless. Facebook has become in effect the world’s largest news agency. Hate speech runs rampant on the Facebook news feed because it engages users, intensifying stereotype-based hatred. It thereby polarizes politics through its near limitless communication platform. Neither social norms nor gate keepers generate restraints while Facebook as a company avoids intervening in contentious exchanges, not to mention engage in censorship. Facebook aims to avoid the inevitable charges of bias from particular frustrated viewers/consumers that inevitably emerge if it employed human managers to attempt to moderate content distribution (Miller, 2018, pp. 184-87). Facebook is a market-share and profit-driven company. Facebook is hesitant to adopt policies that would require it to take public responsibility for inevitably controversial decisions that may drive away some viewers/consumers to other social media platforms.

The Need for Plausible Deniability

The originator of disinformation that is external to the targeted foreign polity must not only be hidden. The disinformation should be depicted as a creation of independent constituencies within the targeted society. Black Elevation is an infamous example of a fake activist group portrayed as the source of social media political advertisements attacking the Hillary Clinton presidential campaign (Frenkel, 2018). This particular feature of the covert Internet-based, Russian government-propagated US influence operation exploited already-present US internal polarization surrounding the Black Lives Matter movement. Escalating social conflict by inciting opposing sides concurrently seemed to be the tactical political objective. Investigative journalism reports underlined the efforts by these Russian state actors to keep their operational efforts hidden.

Misinformation operations disguise their propagator so as to prevent construal of the motives of the initiator which could allow for the perceiver’s dismissal of the misinformation as foreign propaganda. The Russian government’s engagement in these activities derives in part from the Cold War genesis of these programs (Allen & Moore, 2018, Abrams, 2016). Long before Internet-based social media, the requirement to declare the source of initiation of an influence attempt by a foreign government is expressed in the obligation to register as a foreign agent. US law enforcement agencies arrested former Trump presidential campaign manager Paul J. Manafort Jr. for disregarding the 1938 US Foreign Agents Registration Act (FARA), among other charges. Manafort concealed the Ukrainian government as his client sponsoring his firm’s lobbying activities on behalf of pro-Moscow (former) President Yanukovich.

Investigation into the 2016 US presidential has revitalized the heretofore desultory implementation of FARA (Farwell, 2018). Whether such behavior is illegal, not to mention criminal, in a particular case is debatable rather than definitively answerable. A particular case's determination would require that a legal actor with standing have the motivation and resources to support ultimately successful legal proceedings in a court of law with appropriate jurisdiction. E.g., until very recently, US enforcement of FARA was somnolent because the issue of influence generation by foreign actors employing US-based representatives was not a highly salient political issue. Consequently, FARA's requirement to register with the US Justice Department was largely ignored. The 2017 indictment and guilty plea of Manafort and others for violating FARA established a new legal precedent. As a result of the US Department of Justice Special Counsel Robert Mueller investigation, one former official in the Clinton and Obama administrations is under indictment for violating FARA. Mr. Gregory B. Craig has also been charged with failing to register as a Ukrainian government lobbyist (Vogel and Benner, 2019).

Public international law requires that persons employed as agents of influence on behalf of a foreign government must declare publicly their representation. "States have always vigorously protested and claimed compensation when foreign States have exercised on their territory public [i.e. state government-orchestrated (BD)] activities that have not been previously authorized. They have also reacted in this way when the public action on their territory had been performed secretly or by State agents allegedly acting as private individuals" [*sic*] (Cassese, 2005, p. 51). Responding to US government pressure, Facebook today mandates that purchasers of ad space for political purposes confirm that they are US citizens or permanent residents. The pressure on Facebook continues. E.g., in late 2018, a gap in Facebook's new ad policy continued to permit advertisers to fill the "paid for by" field in their advertisements with whatever text they chose. It essentially let them continue to disguise their identity to the viewer. Facebook took the initiative to report externally-based social media influence operations targeting the US 2018 midterm congressional elections as well as other international targets.

Contestants for influence over public opinion in general, and not only international actors, may seek to conceal from view and thereby deceive viewers concerning their instigation of a social action. Political donors may prefer to hide their contributions purposefully if legally feasible: so-called dark money (Ridout, Franz & Fowler, 2015, p. 156). They aim to obscure themselves as the source in order to avoid strategically undesirable interpretations of intent. Thereby, by avoiding disclosure they attempt to generate or support the influence they desire on the audience target of the campaign that they misleadingly support. Research evidence indicates that American voters view so-called dark money, i.e. unattributed campaign financing, as a generally negative feature of a candidate perceived as utilizing such funds (Wood, 2017). Hence, a political candidate for office may seek to obscure their reliance of such campaign resources. Astroturfing is a colloquial term that has become part of the critique of the Internet as camouflage. It refers to misleading attempts to portray grass-roots support online by utilizing the capacities of the Internet to mispresent levels and types of public support for the campaign to the audience. Internet communication generates concern that large organizations disguise their identities to seek "grassroots" credibility for their campaign input in the eyes of their targets, i.e. they "astroturf" (Shafie, 2008, p. 401).

Astroturfing at the international level allows private sector businesses to conceal themselves behind a non-profit, non-governmental organization (NGO) façade, implying broader, humanitarian motivation. It thereby increases their influence within the process of global policy making. Durkee (2017) highlights the challenges of astroturf activism at the international business regulatory level regarding, e.g., tobacco commerce. UN-approved regulations currently forbid for-profit businesses from the formal right of consultancy input into UN international treaty negotiations (p. 206). For-profit corporations manipulate

non-profit non-governmental organizations to mask their covert business input into UN international treaty-making via the formal designation as an UN NGO consultant (Ibid., pp. 243-44). As with astroturfing, this obfuscatory manipulation is not essentially illegal. Such a determination depends not only upon the requirements of a particular legal jurisdiction, but also upon the legal standing, political willingness and financial resources to pursue a legal claim. “Online election campaign speech remains almost entirely unregulated” regarding sponsorship disclosure, illustrating in part the tension with the US Constitution First Amendment’s protection of the right to anonymous speech (Rutenberg, 2019, para. 32).

SOLUTIONS AND RECOMMENDATIONS

First, increase transparency of both governmental and for-profit business influence efforts through international norm-making, e.g. a set of “digital Geneva Conventions” (Sanger 2018, para. 25). “An international lawmaker must be able to identify and rely on the authenticity of the mission the organization pursues in order for the lawmaker to effectively assess that input” (Durkee, 2017, 245). A policymaker should have a plausible opportunity to discern the ultimate, true motivation of an influence organization to evaluate its policy making input. Damage coverage is problematic partly because insurers invoke “war exclusion” to avoid paying costs from cyber combat yet state state-sponsored cyber attackers typically do not publicly declare war (Satariano & Perlroth, 2019, para. 5).

By disguising its real intent or instigation, a political actor in so doing aims to engender the anticipated perceptual and emotional response from the targeted audience (Aakhus, 2016, pp. 202-03). The citizen/media-consumer’s interpretation of the advertisement may otherwise be influenced in an undesirable direction. The perceiver may infer the particularistic, profit-oriented motivation presumed to be motivating a business’ advocacy of a public policy position. Heider (1958[2015]) explained that social actors behave as so-called naïve scientists, prone to attribute and evaluate motives while interpreting the significance of an action by another actor (Harris & Fiske, 2008, pp. 210-11, Körner, Tscharaktschiew, Schindler, Schulz & Rudolph, 2016, pp. 2-3). Judgements concerning the actor’s mental state are intrinsic in comprehending and interpreting social interaction (Vogeley, 2013, p. 297). Political competitors engendering disinformation confront the incentive to disguise their partisan allegiance so that the perceiver is less likely to reject the misinformation for what it is, i.e. partisan propaganda.

According to social psychological concepts of motivational attribution, cognitive dissonance and cognitive balancing, a participant observer will incline subjectively to impute plausible causation to a political act (Pishghadam & Abbasnejad, 2017, p. 137). The concept of transparency mandates cognizance of sponsorship behind a political action. Notwithstanding transparency, the perceiver will likely attribute intent, irrespective of inferential accuracy. Compelling this sponsorship to be public permits the participant observer a plausible opportunity to obtain what they believe to be essential, accurate information. This information is required to attempt plausibly to predict the political consequences of the citizen/media-consumer/participant observer’s own choice of action in response. Through gaining awareness of the source and inferring its motivation, the participant observer interprets the significance of the statement claim. The participant observer accordingly selects their own response to this attempt to persuade this perceiver.

Second, one intent of the European Union’s 2018 General Data Protection Regulation is to restrict the heretofore virtually limitless accretion of individual social media user data. The massive accumulation of this data has been critical for the algorithmic distribution and microtargeting of social media posts. It requires tech companies to receive individual, explicit permission to obtain this private user data. The

activity of covert social media disinformation disseminators would be disrupted, but at a potentially significant collateral damage cost to other lawful and appropriate users, companies and services. Other potential costs include significant barriers to ensuing stages of tech development, including nascent 5G and artificial intelligence-based devices (Radu, 2019).

Third, other proposals include anti-trust action to break up big tech companies such as Facebook (Hughes, 2019). They allegedly now wield monopsony market power that facilitates unethical and illegal systematic and gross privacy data aggregation violations. Covert, hybrid/cyber warfare actors can exploit this aggregated big data for their own particular ends. E.g. Cambridge Analytica, established by a Russian-American academic at Cambridge, constructed social media user profiles from 87 million Facebook users to build microtargeting social media political campaigns. The Trump campaign hired the firm in summer 2016. The April 2019 US Department of Justice report under Special Counsel Robert Mueller on Russian government activity surrounding the 2016 US national elections did not reference Cambridge Analytica (Bertrand, 2019). The perpetually difficult political tradeoffs between guaranteeing security while protecting civil liberties and rights become more complex along with the diffusion of authority over control of information. To resist reasserting this control, obscuring this control becomes politically more desirable. Fourth, a consequent policy response is likely to be a strengthening of the national security establishment's intelligence/counterintelligence capabilities in the form of greater hybrid/cyberwarfare legal competences.

FUTURE RESEARCH DIRECTIONS

Cold War-era American-led influence institutions, e.g. NATO, remain in place. They are developing to respond to new, criminal challenges, e.g. the "cyber ransom attacks" in 2018 against European and non-European institutional targets (Ackerman, 2019, para. 10). US Cold War-era national security institutions command vast resources enabling far-reaching political influence within the US polity. These institutions and their public and private sector support constituencies have vested interests in portraying their existence and role as continuing to be essential for US national security today. These institutions include the covert operations and propaganda bureaucracies that was so much a part of Soviet-American Cold War competition. These assumptions appear to be mirrored in Moscow, i.e. the Soviet-era national security establishment contained the US until poor leadership under Mikhail Gorbachev surrendered to American expansion. Moscow today must use all tools at its disposal to reconstitute its containment effort towards Washington. These tools include Cold War legacies including covert subversion and propaganda capabilities in what is now called hybrid/cyber warfare.

Controlling escalatory crisis dynamics to avoid direct military great power confrontation is essential in the nuclear era. Covert cyberattacks are practical in the nuclear environment because they can be effective and costly to a target but determining their source is problematic and requires much time. Determining responsibility is difficult because indisputable public evidence of the origin of an assault is likely to be lacking. E.g., neither the US nor Israel have confessed to the Stuxnet cyberattack against Iran's nuclear fuel weapons-grade enrichment program, which the Iran authorities never admitted existed. In an illustration of the dangers of blowback, the Stuxnet malware through the Internet then contaminated computer systems outside Iran (Denning, 2012, p. 676). Undeniable evidence of a Pearl Harbor-type surprise cyber-strike would likely generate a nationalist public opinion reaction. Government leaders would then confront the political imperative to select a subjectively determined proportionate response in the era of mass politics. Questions of responsibility remain regarding the destructive 2014 covert

cyber-attack against Sony Pictures Entertainment following release of a film caricature of an assassination plot against North Korea's leader (Brunner, 2017, p. 3 fn. 28). The Obama administration promised retaliatory cyberattack countermeasures but did not specify what they would be or when they would occur (Sharp, 2017, p. 912). Porous state borders in the era of globalization in its latest manifestation in the form of the Internet have expedited intervention in the internal politics of target polities. A likely consequence is the strengthening globally of the intelligence/counterintelligence capabilities and flexible reprisal instruments of the national security state that emerged in the twentieth century in the midst of global conflict.

CONCLUSION

Covert propaganda and influence efforts were a very important part of the so-called Cold War. The US self-perceived success in the containment strategy has led to assumptions and behavior that underplay the progenitors of what is today called hybrid warfare including its cyber component. Covert propaganda disinformation campaigns are not new. Internet social media is new, but it is merely a new vehicle for a familiar policy pattern. The prevalence in the scholarly and news media discourse of heightened alarm regarding so-called hybrid warfare is worthy of research. As noted, the US and the USSR and other actors engaged in this covert, hybrid warfare activity extensively during the Cold War. The collective, selective perception of historical behavior arguably reflects an unwillingness of many in the US to recognize that the US engaged in this form of polarizing activity. Covert propaganda campaigns are hybrid/cyber/dark web warfare when the enemy uses them.

REFERENCES

- Aakhus, M. (2017). The Communicative Work of Organizations in Shaping Argumentative Realities. *Philosophy & Technology*, 30(2), 191-208. doi:10.1007/13347-016-0224-4
- Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal*, 15(1), 5-31. doi:10.11610/Connections.15.1.01
- Ackerman, R. K. (2019, April 1). NATO Cyber Policy under Construction. *Signal*. Retrieved from <https://www.afcea.org/content/nato-cyber-policy-under-construction>
- Adamson, F.B. (2005). Globalisation, Transnational Political Mobilisation, and Networks of Violence. *Cambridge Review of International Affairs*, 18(1), 31-49. doi:10.1080/09557570500059548
- Allen, T. S., & Moore, A. J. (2018). Victory without Casualties: Russia's Information Operations. *Parameters*, 48(1), 59-71. Retrieved from https://ssi.armywarcollege.edu/pubs/Parameters/issues/Spring_2018/9_Allen_VictoryWithoutCasualties.pdf
- Asenas, J.J. & Hubble, B.R. (2018). Trolling Free Speech Rallies: Social Media Practices and the (Un) Democratic Spectacle of Dissent. *Taboo*, 17(2), 36-53. doi:10.31390/taboo.17.2.06

- Bertrand, N. (2019, April 19). 5 Unresolved Mysteries about Russian Meddling in Mueller's Report. *Politico*. Retrieved from <https://www.politico.com/story/2019/04/19/mueller-mysteries-1283775>
- Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., ... Dredze, M. (2018). Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *American Journal of Public Health*, 108(10), 1378–1384. doi:10.2105/AJPH.2018.304567 PMID:30138075
- Bruchmann, K., Koopmann-Holm, B. & Scherer, A. (2018). Seeing Beyond Political Affiliations: The Mediating Role of Perceived Moral Foundations on the Partisan Similarity-Liking Effect. *PLoS One*, 13(8), 1-20. doi:10.1371/journal.pone.0202101
- Brunner, J. A. (2017). The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency. *Jurimetrics*, 57(3), 397–431. Retrieved from <https://search.proquest.com/docview/1965541412?accountid=10373>
- Cassese, A. (2005). *International Law*. Oxford, UK: Oxford University.
- Clogston, J.F. (2016). The Repeal of the Fairness Doctrine and the Irony of Talk Radio: A Story of Political Entrepreneurship, Risk, and Cover. *Journal of Policy History*, 28(2), 375-396. doi:10.1017/S0898030616000105
- Cormac, R. & Aldrich, R. J. (2018). Grey is the New Black: Covert Action and Implausible Deniability. *International Affairs*, 94(3), 477-494. doi:10.1093/ia/iiy067
- Cottam, M. L., & Cottam, R. W. (2001). *Nationalism and Politics: The Political Behavior of Nation States*. Boulder, CO: Lynne Rienner.
- Cottam, R. W., & Gallucci, G. (1978). *The Rehabilitation of Power in International Relations: A Working Paper*. Pittsburgh, PA: University of Center for International Studies, University of Pittsburgh.
- Denning, D. E. (2012). Stuxnet: What Has Changed? *Future Internet*, 4(3), 672–687. doi:10.3390/fi4030672
- DiFonzo, N., Suls, J., Beckstead, J.W., Bourgeois, M.J., Homan, C.M., Brougher, S., Younge, A.J. & Terpstra-Schwab, N. (2014). Network Structure Moderates Intergroup Differentiation of Stereotyped Rumors. *Social Cognition*, 32(5), 409-448. doi:10.1521/oco.2014.32.5.409
- Dunn, A. (2018). *Trump's Approval Ratings So Far Are Unusually Stable - And Deeply Partisan*. Pew Research Center. Retrieved from <http://www.pewresearch.org/fact-tank/2018/08/01/trumps-approval-ratings-so-far-are-unusually-stable-and-deeply-partisan/>
- Durkee, M. J. (2017). Astroturf Activism. *Stanford Law Review*, 69(1), 201-268. Retrieved from <https://review.law.stanford.edu/wp-content/uploads/sites/3/2017/01/69-Stan-L-Rev-201.pdf>
- Farwell, J. P. (2018). Countering Russian Meddling in US Political Processes. *Parameters*, 48(1), 37–47. Retrieved from https://ssi.armywarcollege.edu/pubs/Parameters/issues/Spring_2018/7_Farwell_CounteringRussianMeddling.pdf
- Frenkel, S. (2018, August 15). Real Posts from a Sham on Facebook. *New York Times*, p. B1.

Gaughan, A. J. (2017). Trump, Twitter, and the Russians: The Growing Obsolescence of Federal Campaign Finance Law. *Southern California Interdisciplinary Law Journal*, 27(1), 79–131. Retrieved from <https://ssrn.com/abstract=3069018>

Harris, L.T. & Fiske, S.T. (2008). The Brooms in Fantasia: Neural Correlates of Anthropomorphizing Objects. *Social Cognition*, 26(2), 210-223. doi:10.1521/oco.2008.26.2.210

Heider, F. (2015). *The Psychology of Interpersonal Relations*. Eastford, CT: Martino Fine Books. (Originally published 1958)

Howard, P. N., Ganesh, B., Liotsu, D., Kelly, J., & Francois, C. (2018). *The IRA, Social Media and Political Polarization in the United States, 2012-2018*. Computational Propaganda Research Project. University of Oxford. Retrieved from <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf>

Hughes, C. (2019, May 12). It's Time to Break Up Facebook. *New York Times*, p. SR1.

Isikoff, M., & Corn, D. (2018). *Russian Roulette: The Inside Story of Putin's War on American and the Election of Donald Trump*. New York: Hatchette Book Group.

Körner, A., Tscharschew, N., Schindler, R., Schulz, K., & Rudolph, U. (2016). The Everyday Moral Judge - Autobiographical Recollections of Moral Emotions. *PLoS One*, 11(12), 1–32. doi:10.1371/journal.pone.0167224 PMID:27977699

Lepore, J. (2018, September 16). The Hacking of America. *New York Times*, p. SR1.

Matakos, A., Terzi, E. & Tsaparas, P. (2017). Measuring and Moderating Opinion Polarization in Social Networks. *Data Mining and Knowledge Discovery*, 31(5), 1480-1505. doi:10.1007/10618-017-0527-9

Miller, G. (2018). *The Apprentice: Trump, Russia and the Subversion of American Democracy*. New York: Custom House.

Muggah, R. (2015). The Threat of Organized Crime on Social Media. *World Economic Forum*. Retrieved from <https://www.weforum.org/agenda/2015/07/social-media-violence/>

Ohlin, J.D. (2018). Election Interference: The Real Harm and The Only Solution. *Social Science Research Network*, 1-26. doi:10.2139/ssrn.3276940

Orzeata, M. (2016). Mass Media - An Ally or An Enemy in the Struggle Against Terrorism? *International Journal of Communication Research*, 6(2), 133-42. Retrieved from http://www.ijcr.eu/articole/315_06%20Mihail%20ORZEATA.pdf

Pishghadam, R., & Abbasnejad, H. (2017). Introducing Emotioncy as an Invisible Force Controlling Causal Decisions: A Case of Attribution Theory. *Polish Psychological Bulletin*, 48(1), 129–140. doi:10.1515/ppb-2017-0016

Radu, S. (2019, May 15). Europe's Data Protection Rules Need Reforms, Report Says. *US News & World Report*. Retrieved from <https://www.usnews.com/news/best-countries/articles/2019-05-15/europes-data-protection-rules-need-reforms-report-says>

- Ransom, H. H. (1977). Congress and Reform of the C.I.A. *Policy Studies Journal: the Journal of the Policy Studies Organization*, 5(4), 476–480. doi:10.1111/j.1541-0072.1977.tb01153.x
- Renz, B. (2016). Russia and “Hybrid Warfare”. *Contemporary Politics*, 22(3), 283–300. doi:10.1080/13569775.2016.1201316
- Ridout, T. N., Franz, M. M., & Fowler, E. F. (2015). Sponsorship, Disclosure, and Donors: Limiting the Impact of Outside Group Ads. *Political Research Quarterly*, 68(1), 154–166. doi:10.1177/1065912914563545
- Rutenberg, J. (2019, May 20). The Dark, Faceless Threat to 20 Discourse Online. *New York Times*, p. B1.
- Sanger, D. (2018, June 17). We Can’t Stop the Hackers. *New York Times*, p. SR4.
- Satariano, A., & Perlroth, N. (2019, April 21). Cyberattacks Reveal and Insurance Gray Area. *New York Times*, p. BU1.
- Shafie, D. M. (2008). Participation in E-Rulemaking: Interest Groups and the Standard-Setting Process for Hazardous Air Pollutants. *Journal of Information Technology & Politics*, 5(4), 399–410. doi:10.1080/19331680802546670
- Sharp, T. (2017). Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *The Journal of Strategic Studies*, 40(7), 898–926. doi:10.1080/01402390.2017.1307741
- Shaw, M. (2014). *International Law* (7th ed.). Cambridge, UK: Cambridge University Press.
- United Nations Office on Drugs and Crime. (2010). *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. Vienna: Studies and Threat Analysis Section, Policy Analysis and Research Branch, Division for Policy Analysis and Public Affairs, UNODC. Retrieved from https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf
- Vogel, K. P., & Benner, K. (2019, April 12). Ex-Obama Aide Indicted in Case Linked to Mueller Report. *New York Times*, p. A16.
- Vogeley, K. (2013). A Social Cognitive Perspective on ‘Understanding’ and ‘Explaining’. *Psychopathology*, 46(5), 295–300. doi:10.1159/000351839
- Voss, K. (2016). Plausibly Deniable: Mercenaries in US Covert Interventions During the Cold War, 1964–1987. *Cold War History*, 16(1), 37–60. doi:10.1080/14682745.2015.1078312
- Wilford, H. (2017). American Friends of the Middle East: The CIA, US Citizens, and the Secret Battle for American Public Opinion in the Arab-Israeli Conflict, 1947–1967. *Journal of American Studies*, 51(1), 93–116. doi:10.1017/S0021875815001255
- Wood, A. K. (2017, October). *Show Me the Money: “Dark Money” and the Informational Benefit of Campaign Finance Disclosure*. University of Southern California Legal Studies Working Paper Series. Working Paper 254. Retrieved from <http://law.bepress.com/usclwps-lss/254>

ADDITIONAL READING

- Antonsich, M. (2012). Exploring the Demands of Assimilation Among White Ethnic Majorities in Western Europe. *Journal of Ethnic and Migration Studies*, 38(1), 59–76. doi:10.1080/1369183X.2012.640015
- Blout, E. (2015). Iran's Soft War with the West: History, Myth, and Nationalism in the New Communications Age. *SAIS Review (Paul H. Nitze School of Advanced International Studies)*, 35(2), 33–44. doi:10.1353ais.2015.0028
- Cottam, M. L., Mastors, E., Preston, T., & Deitz, B. (2016). *Introduction to Political Psychology* (3rd ed.). Philadelphia: Routledge.
- Cottam, R. W. (1967). *Competitive Interference and Twentieth Century Diplomacy*. Pittsburgh: University of Pittsburgh Press.
- Cottam, R. W. (1977). *Foreign Policy Motivation: A General Theory and a Case Study*. Pittsburgh: University of Pittsburgh Press.
- Cottam, R. W. (1989). *Iran and the United States: A Cold War Case Study*. Pittsburgh: University of Pittsburgh Press.
- Herrmann, R. K. (2017). How Attachments to the Nation Shape Beliefs About the World: A Theory of Motivated Reasoning. *International Organization*, 71(S1), S61–S84. doi:10.1017/S0020818316000382
- Larson, D. W. (1989). *Origins of Containment: A Psychological Explanation*. Princeton: Princeton University Press.
- Tahjvidi, A. (1997). US Policy Toward Iran: An Interview with Richard Cottam. *Middle East Critique*, 6(11), 5–19. doi:10.1080/10669929708720107

KEY TERMS AND DEFINITIONS

Cold War: Intense bipolar international competition for influence and control between the United States and the Union of Soviet Socialist Republics (USSR). It began at the close of the Second World War and continuing until Soviet-installed communist regimes collapsed in Eastern Europe in 1989 and the USSR itself disintegrated in 1991. This conflict was labelled cold because nuclear weapons made direct military combat between the two likely to result in mutual suicide through escalation to so-called mutual assured destruction. The US and the USSR and their allies and clients therefore competed indirectly through competitive interference in the internal politics of third actors. The Cold War established the template for international conflict between nuclear powers. The cause of US and Soviet conflict is still debated; some argue it was due to mutual fear, others argue that one or the other was bent on imperial expansion, and still others argue that both were bent on imperial expansion. The politically prevailing view in the US today is that the US prevailed over the Soviet Union in the Cold War. Consequently, American-dominated Cold War-formed institutions such as NATO are positive tools for international stability and peace. They should be expanded and adapted to changed circumstances.

Globalization: Increasing global awareness of economic, social and political interdependencies among states due to increasingly porous state barriers due to rapidly increasing commerce, finance, information and labor flows across these borders. Incentives to globalize ultimately relate to the imperative to develop a state's economic and political power resources through integration in the global capitalist production chain.

Hybrid Warfare: A recent term for reliance upon covert and informal policy tools for interference in the internal politics and policy making in target states. This term emerged concurrently with the development of the Internet as an infrastructure vehicle and as form of media communication. Covert and informal modes of international political competition and influence expansion acquired greater emphasis along with the post 1945 nuclear setting. The need to maximize the degree of control over potentially escalatory conflict dynamics pushed policy makers to obscure their international victories, defeats and stalemates in order to lessen the potential for provoking nationalist hostility that would lessen the political decisional latitude available to policy makers.

Nation: A community which a nationalist believes should and can achieve national self-determination through acquiring a sovereign state for the nation if it does not already have such a state. If this community already has its own sovereign state, then the nationalist will be perceptually and emotionally preoccupied with challenges to this sovereign state, tending to equate the state, represented by its governmental apparatus, with the nation.

Nation State: A state in which the overwhelming majority of citizens show their primary self-identification with the territorial community within the state through favoring it more above any other identity group or community. Examples include the United States, Russia, China, Japan, Germany and others. Multinational states, such as the old Soviet Union and Yugoslavia as well as Iraq, are not nation states. Neither are multiethnic states nation states. Examples of the latter include most post-colonial African and many post-colonial Asian states including India. Non-nation states, and multinational states in particular, are subject to centrifugal political forces among ethnic groups seeking national secession and self-determination. These centrifugal forces may maintenance of liberal democratic political regimes highly problematic insofar as democratic elections produce ethnic nationalist leaders seeking self-determination. The communities of the old Yugoslavia as well as in the old Soviet Union continue to deal with such secessionist and irredentist nationalist forces.

Nationalism: A form of intense ingroup political loyalty opposing perceived challenges to the sovereignty of the nation. It is characterized by relatively intense emotional affect and perceptual stereotyping of self and other, outgroups stereotypically perceived as challenges to the nation. A community behaves nationalistically when the modal, politically attentive citizen is a nationalist.

Nationalist: An individual who sees himself/herself as a member of a large group of people who constitute a community that is entitled to independent statehood and who is willing to grant that community a primary and the primary terminal loyalty.

Polarization: Intra-societal stereotyping due to intensifying perceived challenges from other constituencies within a polity, with the different contestants portraying the other as disloyal, even treasonous, to the nation and its state. Polarization is most likely to intensify when certain constituencies within the polity portray their favored policy prescriptions for the perceived well-being of the nation as religiously, i.e. divinely mandated. Secular opponents, therefore, are more likely to be stereotyped as evil and disloyal.

Power: The exercise of influence over the minds and actions of others.

Stereotype: A simplified perception of the political environment, specifically regarding policy targets. Differences in stereotypical patterns in perception emerge along with different types of perceived challenges to the perceiver from a target. An intensely threatening target of perceived equal capability and techno-cultural level will tend to be perceived as a diabolical enemy. A perceived weak, inconsistent and unmanageable target unable to resist the perceiver's greater will and determination to achieve its objectives will tend to be perceived as degenerate. Dangerous adversaries perceived as superior in capability and techno-cultural capabilities will tend to be perceived as an imperial threat. Perceived weaker targets in capability and culture ripe for exploitation to achieve some other overarching objective, i.e. containment of a great power enemy, will be perceived as a colonial target of opportunity. Troublesome, threatening weaker targets in culture and capability will tend to be perceived as criminal rogues.

The Spy Who Never Has to Go Out Into the Cold

Cyber Espionage

Laura Pinto Hansen

Western New England University, USA

INTRODUCTION

Cyber espionage is a fairly recent newcomer to means by which to steal trade secrets, classified government information, or consumer information. However, with the rise of the digital age beginning in the late 1950s, increasingly more documents are stored on mainframe and individual computers than compared to storage in conventional file cabinets. In fact, it is very unlikely that many institutions store files these days on physical shelves, save older archives. Even then, the art of archiving reached the digital age some time ago. This has been exponentially so since the beginning of the Big Data age of the 21st century. In this chapter, we explore the types of cyber espionage, recent cases, as well as challenges to detecting, controlling cyber thievery and mayhem.

It is because of the vast amounts of data that are stored more efficiently on computers and in cyberspace, that these became the new frontiers for spies. Banks (2017, p 513) observes that “it seems that everyone is eavesdropping on everyone else...” Gone is the heyday of trench coat wearing spies wielding mini spy cameras in corporate headquarters, the stuff of Hollywood movies. Dark alley, middle of the night transactions, passing microfiche, audio tapes or video, or files, became increasingly unnecessary with the ease and speed of computer technologies.

A circular tautology exists: Technology has always created new advances in warfare (Roberts, 2017) and new advances are created during times of war, including in those conducted in cyberspace. Even art imitates life, with movies depicting elaborate fictional cybercrimes that are not so far-fetched. A handful are even based on true cases, as in the 2013 movie, *The Fifth Estate* (DreamWorks), depicting the infancy of the website, WikiLeaks.

Spying is considered business as usual in international relations, though nations publicly deny that they are involved in espionage. State-sponsored surveillance is common place and considered to be a necessary evil in order to maintain world order and promote national security. This challenges the principles of democracy and privacy. State-sponsored surveillance has its critics (Schmitt and Vihul, 2017). Comparisons have been made to George Orwell’s 1948 novel, *1984*, where Big Brother is always watching: “If you want to keep a secret, you must also hide it from yourself.” (Orwell, 2017, p 283)

On the other side of the argument, surveillance is argued to be a necessity in order to detect cyber attacks (Nissenbaum, 2005). The consequences of cyber intrusions by perceived hostile nations or “frenemies” (nations who are friendly for purposes of trade relations, but secretly economically and militarily compete with) are far reaching. As much as state-sponsored surveillance of governments is

commonplace, surveillance and cyber espionage are more likely to have an effect on the average citizen, much like other forms of white-collar crime, as compared to conventional crime. In many respects, there is far greater financial and political damage to be done in this day and age, because of the alarming amounts of sensitive information that is stored digitally.

More recent attention has been given to the ability to plant false information through the Internet, in order to engage in propaganda designed to confuse or divide nations' citizens. There is also the greater concern that whole cyber infrastructures could come tumbling down, with the ability of cyber spies or amateur hackers to infiltrate systems for purposes of sabotage, including energy and transportation.

DEFINING CYBER ESPIONAGE

As Randall Dipert (2013) argues, the terms “cyber attack” and to some extent, “cyber espionage” are loosely interchangeable, used to cover a wide range of cybercrimes. We should be clear that cyber espionage is more commonly thought to be limited to the theft of military or government secrets. A subset of cyber espionage is economic espionage, sometimes called industrial espionage, where governments attempt to gain information from foreign companies (Banks, 2017). A cyber attack or cyber warfare, on the other hand, implies that the act is for the purposes of bringing down whole systems, as in the example of viruses transmitted by bogus links imbedded in spam email.

One common means by which to obtain information from individuals is phishing. It is not restricted to attempts to gain personal financial information from employees. In recent decades, the use of company email exchanges has commonly been used to gain access to intellectual property and industry secrets. These are not easily detected schemes, as compared to the notorious Nigerian email scams. Increasingly the emails appear to be generated from legitimate sources, addressing employees by name within an organization, rather than the generic “Dear Sir or Madam”. Sometimes initiated on the Dark Web, it is an effective way to gather information without hacking into sophisticated computer systems that might be heavily protected by more sophisticated cybersecurity systems. And because many are distributed through the Dark Web, the origins of the emails are difficult to detect. The Dark Web allows users to mask not only their identities, but their location.

Cyber espionage is not always limited to the theft of intellectual property. Espionage can also involve subterfuge where false or misleading information is planted. The most common current means by which to do so is through social media, including Facebook, Twitter, Instagram, and YouTube. Though these social media platforms have battled regulatory agencies to offer open access with few limitations, increasingly they have been asked to take a more active role in preventing foreign agents, acting as internet trolls, from agitating users, particularly during election cycles.

An additional form of cyber espionage is the use of malware for intelligence gathering and sabotage. These might not be isolated incidents, but rather can be ongoing campaigns by their designer, attacks presenting themselves within an advanced persistent threat (APT) (Wangen, 2015). Malware can come in a number of different forms, including temporary nuisances, as in the case of “bugs” or having far more devastating result, as in the example of a “Trojan horse”. More commonly in cyber espionage, the use of spyware allows for information to be collected from individual computers, including keystrokes to obtain passwords or gather information about use. The lesser known, but in many respects, deadlier “rootkit”, allows the user to evade detection and has the ability to alter software, including security systems.

Unlike the stereotype of the lone hacker or spy working from some dank basement apartment, much of what is occurring is within criminal networks. Social network theories are excellent tools in order for researchers to understand the mechanics, beyond the technical, of how cybercrimes, including espionage, are executed (Schaefer, 2014). The targets of criminal networks conducting cyber espionage vary and can include a number of illegal activities. Some of the types of illegal activities can be found in Table 1.

The fact that cybercriminals can operate within a network, once detected, they run the risk of exposing other members of the network to detection. However, as is the case with criminal and legitimate social networks, the boundaries of a network can be vague (Hansen, 2009). This makes it difficult for law enforcement agencies to capture every actor within an illegitimate network. What is particularly challenging and aggravating to investigators is that criminal networks can be embedded within legitimate networks (Hansen, 2009).

Historically, a criminal is physically present at the crime scene (Speer, 2000), allowing in some cases for law enforcement to apprehend a perpetrator on the spot, catching them in the act. This is particularly true in undercover sting operations. Now a corporate or government spy doesn't even have to leave their home, much less their country, to gain access to digitally stored information. This has never been more evident than with the infamy of Julian Assange, mastermind behind WikiLeaks, an international non-profit organization dedicated to publishing classified documents and information for alleged altruistic reasons and purposes of government transparency. Though arguably, detection is not impossible, and may cause the perpetrator to go on the run to avoid capture. As a direct result of Assange's activities, he is man without country at the moment, holed up in the Ecuadorian embassy in London as of this writing. But his nomadic existence does not stop him from continuing his operations.

CYBER ESPIONAGE AND INTELLECTUAL PROPERTY RIGHTS

There is an ongoing battle between advocates of the preservation of intellectual property rights and the demand for freedom of information by others. This is especially typical in democratic societies, as exemplified by the Freedom of Information Act in the U.S. (FOIA). As we have shifted from an industrial

Table 1. Seven forms of information warfare

TYPE	DESCRIPTION
Command-and-control	Attacks on command centers or commanders themselves to disrupt command effectiveness
Intelligence-based	Increasing your own situational awareness while reducing your opponent's
Electronic	Using cryptography and degrading the physical basis for transferring information
Psychological	Propaganda to demoralize troops or influence civilian populations
Hacker*	Exploitation of viruses, etc., to attack computer systems
Economic Information	Possessing and being in control of information leads to power
Cyber	Information terrorism
*We should note that the term "hacker" is now used to include individuals who infiltrate computer systems legitimately, the so-called "white hats", to understand and detect vulnerabilities.	

Sources: Libicki, 1995; Robinson et al., 2015, p 7

economy in the U.S. to an economic dependence on the buying/selling of information and services, it has been a daunting challenge to protect the intellectual property rights of individuals and corporations.

For all the legal considerations, a war is being waged between advocates of open, free-flowing access to intellectual property and those who argue that intellectual property should be protected. Intellectual property can include copyright protected materials, patents and research that is in its infancy should be closely guarded in order to give credit where credit is due. For example, a pharmaceutical company would not want released to the public the results of drug trials in advance of Federal Drug Administration (FDA) approval or rejection. Stock prices rise and fall on the basis of the success (or in some cases, failure) of drug trials.

To further complicate matters, the divide is between the desire for accountability and the demand for privacy (Moore, 2017). In an age of personal information being commodified, bought and sold on the open market, some question whether the concept of privacy has met its extinction in the 21st century. Standing in the way of free access is a litany of U.S. copyright, patent, and trade secret laws (Moore, 2017) that may or may not make sense in a contemporary free-market system.

This begs the question as to whether the stealing of trade secrets is quasi-legal, similar to the ambiguity of insider-trading regulations. Clearly the theft of industrial secrets outside of those associated with national security are more likely to cause financial loss rather than threatening government institutions, except in the case of the defense industry. As much as financial losses can be devastating, of graver concern is the protection of industrial secrets and information associated with military equipment and personnel. Hence the paramount drive to protect intellectual property that involves national security, in spite of claims that all intellectual property should be freely open to the public, not only at the expiration of copyrights and patents.

Further support for the claim of ambiguous regulation is that digital piracy has been difficult to specifically define, much less regulate. Earlier definitions of piracy only included the illegal duplication of computer software (Higgins, 2014; Koen and Im, 1997; Straub and Collins, 1990). However, more recent definitions include a number of crimes, including the theft of digital documents and digital audio or video that is copyrighted (Higgins, 2014).

Speculating on the merits of protecting intellectual property rights is all well and good. However, putting this in context of a global market with global competitors, international attitudes towards rights vary. In some cases, the adages “all’s fair in love and war” and “what is mine is mine; what is yours is mine, if I can take it away from you” makes some intellectual property laws impotent. It has been estimated that upwards to 25% of computer software alone is pirated in the U.S.; on the high end, 81% is pirated in Thailand, with the mean global piracy rate at 36% (Moore, 2017). And that is just in one industry. This represents billions of dollars (USD) lost in software piracy alone, not to mention legal costs when pursuing justice through civil court systems.

Of greatest concern about the loss of intellectual property is the maintenance of stable world order. Scholars and practitioners argue that countries must develop and maintain means by which to preserve international legal order, to assure that security and stability are maintained (Schmitt and Vihul, 2017). There is little understanding of how international law prior to the computer age can be applied to emerging technologies. The institution of law is slow moving, whether interpreted by national or international standards, and cannot necessarily keep up with the rapid march of new technologies. The old adage (Schmitt and Vihul, 2017, p xxv), “*inter arma enim silent leges* – ‘In times of war, the law falls silent’” may apply here as well, as some would argue that we are currently in the age of ongoing cyber wars. But it begs the question, can a cyber attack that includes the theft of intellectual property be considered an “armed attack” (Roberts, 2014) warranting the self-defense of the targeted victim?

TARGETS OF CYBER ESPIONAGE

Cyber espionage targets include a wide range of economic sectors, including energy, finance, IT, aerospace, and biotechnology (Nakashima, 2013). Currently the United States, as one of the economic leaders in the world, is perceived to be the biggest target of cyber espionage. Though certainly it is not the only country that has more recently had to deal with theft of intellectual property or cybersecurity breaches. For example, Tibetan institutions have also been on the receiving end of cyber espionage, as China views cyberspace a strategic platform on which to level military imbalances (Delbert and Rohozinski, 2009). Nevertheless, the U.S. has been repeatedly been targeted by China and others.

The U.S. is not simply an innocent victim of cyber espionage. The United States, along with Russian and China, are viewed as possessing the most technically advanced cyber spies. As noted elsewhere in this chapter, cyber espionage is part of the new Cold War fought in cyberspace.

Individuals, including journalists and politicians, are also seen as targets for surveillance, sometimes by their own governments. There is the expectation that there will be more attacks on and surveillance of individuals by nation-states, as alleged in the case of Saudi journalist Jamal Khashoggi (CSO, 2018).

It cannot be assumed that just because a country allows limited access to the Internet within its borders that cyber espionage can't or doesn't take place. Though more rural locations may have no or limited access to the Internet, governments are assumed to be highly connected. And not all cyber espionage is conducted through more transparent network means. As long as there is a black market for sensitive information, transactions will continue to take place on the Dark Web, an underground network existing on the Internet that requires more sophisticated software and authorization to gain access, offering anonymity to users.

Organized crime is also a contributing factor in cyber espionage. Organized crime, is operating both on the streets and in cyberspace, and function like legitimate, bureaucratic business structures. The fact that cyber conspirators in organized crime are now scattered across the globe allows for more flexibility in operations (Fielding, 2017). As noted earlier, social networks are a natural conduit in which to conduct criminal acts, including organized crime in cyberspace.

Though organized crime groups are ordinarily thought to deal in conventional victimless crimes like loan sharking, drugs, and prostitution, by definition, any group that is powerful and is able to conduct sophisticated criminal operations, including cybercrime, can be considered part of organized crime. And as cybercrime, including espionage, is so lucrative, it makes sense that more traditional organized crime groups would look to see this as the new marketplace for illegal activities, operating as a "cyber mob" (Armerding, 2015).

Universities, especially those focus on research (e.g Massachusetts Institute of Technology), are increasingly more vulnerable to cyber espionage. As universities are viewed as industry partners in a number of sectors, including national defense and biomedicine, they are a ripe target for attack from an insider or outsider. More commonly the threat is to student data, including social security numbers. Because of the number of international students attending prestige, Tier 1 research institutions, there is the risk for students and even faculty in all fields to steal science, including unpublished research (Reisch, 2018). With China's military apparatus cited as one of the biggest culprits, there are hundreds of thousands of attempts made to breach university systems on a daily basis (Rogers and Ashford, 2015).

CYBER WARS

2

Cyber warfare, along with a number of topics discussed in this chapter, is difficult to define. In fact, the term is very broad and may include a number of different types of attacks, including intelligence-based, and information terrorism (Libicki, 2016; Robinson et al., 2015). A comprehensive list of Libicki's typologies of cyber warfare can be found in Table 1.

One of the chief concerns of all nations beyond protection of classified information, is national security of any and all infrastructures that are dependent on computer technology. Cyber espionage can include sabotage. There is the real possibility that a foreign government could hold another country hostage by infiltrating or destroying critical computer infrastructures. Everything from electric grids to flight operations are controlled with computers and the fear is that sooner or later, instead of a nuclear attack, a country could come to a full stop by a cyber attack. And cyber attacks on infrastructures have the potential of doing far greater long-term harm, than in the cases of garden variety viruses or unauthorized computer break in, as these take longer to recover from (Nissbaum, 2005).

Additional serious concern is any cyber attack that specifically target transportation or energy, is that government agencies, industries, medical facilities, and first responders are dependent on these being up and running at all times. Emergency response teams have a challenging time responding to natural or human-made disasters, even when transportation and electric grids are minimally impacted.

So far, devastating human generated attacks that have the potential of directly affecting millions of citizens have been thwarted on the most part. A successful large-scale attack is not an impossibility, as in the example of the 2015 service outages in the Ukraine, that Ukrainian officials attribute to Russian security services, (Lee et al., 2016). The belief is not *if* a widespread power outage due to cyber attack will happen, but *when* and *where* it will happen. Large scale attack could throw a portion of the world into 19th century conditions, something that some governments and most individuals are ill-equipped to handle. Fortunately, due to the interdependency of the world economy where it would not be in nations' self-interest to engage in widespread cyber warfare, it is unlikely that this will happen in the foreseeable future.

More recently attention has been given to cyber espionage and warfare in the form of political propaganda and manipulation, as in the ongoing Robert Mueller investigation into alleged election tampering and voter suppression. Mueller was named by the Justice Department to head the FBI's special counsel investigation of the 2016 Presidential election in the United States. Allegedly, at the time of this writing, the espionage was being condoned by highly placed individuals in the Russian government. Beyond the leaking of supposedly compromising information about Hillary Clinton, Donald Trump's opponent in the election, there is currently an investigation into other alleged improprieties, including cyber espionage. As of this writing, a comprehensive report from the Mueller team is pending and the investigation is ongoing.

Is it even possible for social norms, beyond laws, to control free speech that is aimed at political manipulation and fraud? There is the misguided trust that all internet consumers can distinguish between what is fact and what is fiction. A Pew Research Center study found that 64% of American adults believed fake news stories during the 2016 election campaign cycle, with 23% reporting that they shared the stories online (Anderson and Rainie, 2017). Because of these events, democratic governments are now taking an active role in holding social media outlets responsible to curb any interferences that might influence the outcome of an election.

Though changes in technologies create new challenges to the First Amendment rights to free speech and free press, this does not mean that efforts to protect it should be abandoned. Wu (2018, p 550) cautions that “we need recognize the role and, indeed, the duty of those who enforce the laws to uphold the First Amendment by defending the principal channels of online speech from obstruction and attack, whether by fraud, deception, or harassment of speakers.”

In light of the current Mueller investigation and the rise of concerted efforts to infiltrate social media, including Facebook, during elections, the First Amendment rights to free speech and free press, as they are currently spelled out in the U.S. Constitution, are being questioned. With its original intent restricted to print media, the uncharted territory of whether it should apply to the more insidious speech filtered through social media. Though it could be argued that this is not decisively different than yellow journalism of the early 20th century, just more widely consumed. As always, the jurisprudence of the First Amendment is caught between the proverbial rock and a hard place.

COSTS OF CYBER ESPIONAGE

As in the case of white-collar crime in general, the financial losses to individuals, banks, corporations, and governments far exceeds the losses from conventional crime. Estimates run in the tens of billions (Nakashima, 2013). Estimates from global cyber activity are losses of between \$300 billion to \$1 trillion (USD), with \$24 billion to \$120 billion (USD) attributed to the U.S. alone (Center for Strategic and International Studies, 2013). In addition to direct costs, there are the exorbitant costs associated in securing networks and hiring cybersecurity personnel, not to mention updating and upkeep of software.

Beyond direct and indirect monetary losses and costs, cyber espionage results in the loss of untold volumes of government and business information, including military secrets, intellectual property and data on customers. A list of high-profile cases of cyber espionage can be found in Table 2. In some cases, loss of intellectual property can negatively affect stock prices for publicly traded companies. In other cases, the real costs, monetary and otherwise, are unknown, including costs to national security. As in other types of white-collar crime, cybercrime can also tear at the social fabric, creating distrust in governments and economic institutions. This has certainly been witnessed in a number of thefts of customers' financial information in recent years from retail companies in the U.S., including Macy's and Sears department stores.

CHALLENGES TO INVESTIGATING AND CONTROLLING CYBER ESPIONAGE

There are a number of ongoing threats to cybersecurity, as well as new ones looming on the horizon. With the growing popularity of authentication, it is predicted that biometric hacking in healthcare, government, and financial institutions will be on the rise (Nadeau, 2018). Encryption alone does not prevent cyber spies from obtaining sensitive information. The Deep Web, that theoretically acts as a locked vault for financial and personal information, does not guarantee that data will not be stolen, as in the examples of identity theft and financial data.

Table 2. 10 biggest cyber espionage cases

YEAR(S) DETECTED	TARGET	CRIME	SUSPECT(S)
1999	Wright Patterson Air Force Base	Stolen American military research documents	Russians, but no proof
2003-2007	U.S. government computers	Stolen intelligence	Chinese military hackers
	UK defense ministries		
1997	Design technology	Stolen intellectual property	Steven Louis Davis
2012-2017	Personal information of government employees	Cyber attack	Allegedly Chinese Government
2010	Google, including Gmail accounts	Stolen intellectual property	Allegedly Chinese spies
2009	Computers in 103 countries,	Unauthorized access	
	Foreign ministries and embassies	Cyber attack	Allegedly Chinese government
2011	European and American energy businesses		Chinese hackers
2008	Computers of the two presidential candidates	Data leakage, cyber attack by computer virus	Allegedly Chinese or Russian hackers
2009	Intelligence on next generation fighter jets	Stolen data	Computers located in China
	Electronic and maintenance information		
2006	A number of international companies	Distribution of malware, stolen intelligence	Allegedly Chinese spies
	and organizations		

The ongoing concerns of cybersecurity are not limited to law enforcement and regulatory agencies. Though cybersecurity is an exponentially booming industry, an understanding of what cybersecurity exactly entails is still not clear (Parekh et al., 2018). And as the government, corporations, and institutions (e.g. colleges and universities) may be constrained by budgetary concerns, they may not be able to purchase ample cybersecurity nor hire adequate numbers of specialists to maintain and monitor systems in place.

It is particularly important to note that as in the case of conventional crime, resources for combatting cyber espionage are focused more on control rather than prevention. As Speer (2000) noted during the infancy of cybercrime research, domestic and international security agencies shifted attention away from espionage towards transnational criminal threats, including drug trafficking and organized crime, after the Cold War, as they became more high profile. This left vulnerabilities in the prevention of cybercrime, as resources were spread thin elsewhere.

One key to investigating cyber espionage is to not only understand computer networks but also understand the uses of social networks to commit cybercrimes. Exploitation of unsuspecting victims is predicated on developing trust relationships. More alarming is that espionage activities are not limited to relationships between sophisticated, trained spies. During the 1990s, an Israeli operative helped a couple of teenagers in California interfere with military deployments (Speer, 2000).

An act of espionage is not always an outside job. As in the case of traditional espionage practices, trusted employees are still utilized in order to steal secrets (Duckworth and de Silva, 2016). A second critical issue beyond the extent that social networks play a part in espionage activities, is the concern that blackmailed personnel may give up trade secrets or sensitive information. It is the very reason that individuals who handle sensitive data are asked to undergo extensive background checks, including investigation into financial history, as someone who is in serious debt or financial trouble can be made a target of blackmail or corruption.

Blackmail is, per se, nebulously illegal, as in the case of other victimless crimes (e.g. prostitution). Even though the blackmail target may feel that they have no choice but to comply with the blackmailer, it is a relationship that is viewed to have been entered into voluntarily, between consenting adults (Block, 2000). Unless the targeted victim comes forward to authorities, blackmailing activities can be ongoing. There is little incentive for the victim to come forward, as in the process of paying the blackmailer in embezzled funds or information, as they may very well be committing a crime themselves.

An additional weakness in cybersecurity is that there is a tendency towards general deterrence that does not always help in protecting systems against specific threats. As Duckworth and de Silva (2016) caution, security personnel are more likely to take an agnostic, whole system approach to protection, with less focus on who or what is threatening their systems. However, in the defense of security experts, it is a challenge for cybersecurity specialists to keep up with the vast number of means that cyber espionage can be accomplished, much less the direction it is coming from. This is particularly true with the ability to conduct cyber espionage anywhere with the country of origin in question.

An additional major drawback in investigating cyber espionage is that a growing number of cases involve foreign governments, making detection and regulation challenging, not to mention diplomacy. And because regulation requires legislation, by the time that laws have been enacted, some have already become obsolete, particularly those that target specific types of cybercrime. There is the question of cooperation and challenges to jurisdictional law when trying to control cyber espionage that crosses international borders. As we have witnessed in the Assange case, it is not always easy to stop theft and bring the accused to justice, when foreign governments do not cooperate in doing so.

Recent research indicates (Haider, 2018) that there are some countries that may wittingly or unwittingly contribute to cyber espionage by the nature of their legal systems. It is no secret that embassies and consulates operate with a different set of laws than the national soil that they occupy. However, some countries are more restrictive of the activities operating out of the embassies and consulates of foreign countries. Select countries have even been accused of harboring spies, as in the example of the “repeated claim of Austria being a hot spot of international espionage activities.” (Haider, 2018, p 201)

Beyond complacency of foreign governments, there are some that have a more visible reputation than others for conducting cyber espionage. For example, in 2014 the FBI issued a list of “Most Wanted” Chinese nationals, alleged members of the People’s Liberation Army who were indicted for stealing trade secrets for the benefit of Chinese companies (Banks, 2017). And as noted by Table 2 on the ten biggest cases of cyber espionage, China is allegedly the worst offender, though this may be difficult to prove empirically.

As recently as December 2018, Chinese nationals are being accused by the U.S. Justice Department of a global scheme to steal business and military secrets (Isidore and Gaouette, 2018). Among the charges are stealing names, Social Security numbers, salary information of naval personnel. According to Isidore and Gaouette (2018), efforts to bring charges were aided by a number of countries. The value in global cooperation in combating cyber espionage is in pooling otherwise limited resources.

The good news is that cybersecurity against espionage is not completely impossible. There are a number of measures that are in place, including new laws and agencies to deal with the advances of technology. Additionally, there is more focus on employee training in order to make them aware of possible cyber threats within their organization. Plus, as a growing niche employment market, universities are churning out more graduates in IT and CS specializing in cybersecurity. The Bureau of Labor Statistics projects that there will be a 28% increase in demand for information security analysts in the future, a much faster than average growth rate, as compared to other occupations (BLS, 2018).

One measure, among many, that the U.S. federal government has recently taken, is Executive Order 13010 under President Bill Clinton (1996). The executive order called for strategies to protect sensitive infrastructures from cyberattacks with the creation of the Federal Intrusion Detection Network (FEDNET) (Speers, 2000). However, the focus of the new agency was on malicious activity, rather than on attempts to stem the theft of intellectual property or sensitive government data, as FEDNET is intended to protect cyber infrastructures.

As in the case of white-collar crime in general, employers can also put preventative measures in place, beyond cybersecurity. Though not always within the control of supervisors, compensation packages should be perceived by employees to be adequate and competitive for their professions (Hansen, 2009). Employees are vulnerable to corruption if they believe that they are inadequately compensated by their employers for their labor. Employers should also be cognizant of the informal social network dynamics within their organizations, as these may supplant any formal hierarchy structures (Hansen, 2009). These measures should be the responsibility of not only chief security officers (CSOs), but of supervisors and upper level administrative personnel.

One of the strongest weapons in combating cybercrime is public sentiment. In 2017, Equifax, a company that provides credit information and ratings to lenders, had a major breach where approximately 150 million people may have had their personal data exposed. With a number of breaches of credit card information in recent years, the public is much more aware of the risks of having their personal data stolen, resulting in demand for secure data. This does not translate to greater demand for cyber security to prevent the theft of intellectual property. However, public sentiment is predicted to drive data protection policies and pushes for more regulation (CSO, 2018).

FUTURE RESEARCH CONSIDERATIONS

The weaknesses in thinking about the direction that cyber espionage research should go are the same as with white-collar crime research in general. Much of what we can do researching this niche of white-collar crime is to mine news accounts, within historical context, or anecdotal ethnography. Prediction and prevention are near impossibilities, beyond general cybersecurity, making inferential research problematic. The crux of the matter is that as soon as the latest methods by which cyber espionage is committed is discovered, the perpetrators are cooking up newer, better technological *modus operandi* by which to infiltrate vulnerable computer systems.

For scholars, an additional challenge is in coming to a consensus of definitions, whether discussing cyber espionage, cyber attacks, or cyber warfare. Social sciences are in a unique position in doing this type of research in shaping definitions for future consideration, as there is the necessity to include research from the “hard sciences”, including information technology (IT) and computer science (CS). Any future considerations for research on cyber espionage within criminologist circles should consider including cross-discipline collaboration with scholars in IT and CS.

Certainly, more research needs to be conducted taking a global perspective. The world is increasingly more connected by way of computer networks in the 21st century, even in some of the more remote or less developed places on the globe. More commonly, there are a number of countries with restricted or limited internet access, including North Korea, Egypt, and Iran, that are by no means excluded from more advanced computer technologies. The ongoing drawback in approaching cybercrime from cross-national comparison is that there are a number of countries that are not forthcoming with crime statistics, as in the example of North Korea. Likewise, attitudes towards what is permissible in cyber activities to secure economic viability in the world economy, as well as national security, varies drastically across the globe.

All in all, beyond the practical applications resulting from any examination of cyber espionage, it is a great opportunity to update somewhat stale white collar crime research for the 21st century. We have only scratched the surface in social science research in cyber crime. Scholars and practitioners will have to be equally adaptable to technological change, as the cyber spies themselves are becoming more sophisticated in their methods.

REFERENCES

Anderson, J., & Rainie, L. (2017). *The future of truth and misinformation online*. Pew Research Center, Internet and Technology. Retrieved from <http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/>

Armerding, T. (2015). *Cybercrime: Much more organized*. CSO, IDG Communications, Inc. Retrieved from <https://www.csoonline.com/article/2938529/cyber-attacks-espionage/cybercrime-much-more-organized.html>

Banks, W. C. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory Law Review*, 66(3), 513–525.

Block, W. (2000). Threats, blackmail, extortion, and other bad things. *Tulsa Law Review*, 35(2), 333–351. Retrieved from <https://digitalcommons.law.utulsa.edu/cgi/viewcontent.cgi?article=2218&context=tlr>

CSO. (2018). *9 cyber security predictions: Our hopes (and fears) for the infosec world for the coming year*. CSO, IDG Communications, Inc. Retrieved from <https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html>

Duckworth, N., & de Silva, E. (2016). In I. G. I. Global (Ed.), *Teaching new dogs old tricks: The basics of espionage transcend time*. In *National Security and Counterintelligence in the Era of Cyber Espionage* (pp. 76–95). doi:10.4018/978-1-4666-9661-7.ch005

Fielding, N. G. (2017). The shaping of covert social networks: Isolating the effects of secrecy. *Trends in Organized Crime*, 20(1-2), 16–30. doi:10.1007/12117-016-9277-0

Haider, I. (2018). Austrian law as a safe haven for foreign spies?: Analysis on the recent phenomenon of ‘Embassy Espionage’. *European Journal of Crime Criminal Law and Criminal Justice*, 25(3), 201–221. doi:10.1163/15718174-02603002

Hansen, L. L. (2009). Corporate financial crime: Diagnosis and treatment. *Journal of Financial Crime*, 16(1), 28–40. doi:10.1108/13590790910924948

- Higgins, G. E. (2014). Understanding digital piracy using social networks. In C. D. Marcum & G. E. Higgins (Eds.), *Social Networking as a Criminal Enterprise*. Boca Raton, FL: CRC Press. doi:10.1201/b16912-10
- Isidore, C., & Gaouette, N. (2018). US charges Chinese hackers in global scheme targeting business and military. *CNN*. Retrieved from <https://www.cnn.com/2018/12/20/tech/chinese-hacker-charges/index.html>
- Koen, C. Jr., & Im, J. H. (1997). Software piracy and its legal implications. *Information & Management*, 31(5), 265–272. doi:10.1016/S0378-7206(96)01090-7
- Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. Electricity Information Sharing and Analysis Center (E-ISAC). Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
- Libicki, M. (2016). *Cyberspace in peace and war*. Annapolis, MD: Naval Institute Press.
- Moore, A. D. (2017). *Intellectual Property and Information Control: Philosophic Foundations and Contemporary Issues*. Philadelphia, PA: Taylor & Francis Publishers. doi:10.4324/9780203788400
- Nadeau, M. (2018). *Data breach predictions for 2019*. CSO, IDG Communications, Inc. Retrieved from <https://www.csoononline.com/article/3328396/data-breach/13-data-breach-predictions-for-2019.html>
- Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, 7(2), 61–73. doi:10.1007/10676-005-4582-3
- Orwell, G. (2017). 1984. Boston, MA: Houghton Mifflin Harcourt.
- Parekh, G., Delatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2018). Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education*, 61(1), 11–20. doi:10.1109/TE.2017.2715174
- Reisch, M. S. (2018) Acknowledging the spies on campus. *Chemical and Engineering News*, 96(27). Retrieved from <https://cen.acs.org/policy/intellectual-property/Acknowledging-spies-campus/96/i27>
- Roberts, S. (2014). Cyber wars: Applying conventional laws of war to cyber warfare and non-state actors. *Northern Kentucky Law Review*, 41(3), 535–572.
- Robinson, Jones, & Janicke. (2015). Cyber warfare: Issues and challenges. *Journal of Computers and Security*, 49, 70-94.
- Rogers, G., & Ashford, T. (2015). Mitigating higher ed cyber attacks. *Association Supporting Computer Users in Education Conference Proceedings*.
- Schaefer, B. P. (2014). Social networks and crime: Applying criminological theories. In C. D. Marcum & G. E. Higgins (Eds.), *Social Networking as a Criminal Enterprise*. Boca Raton, FL: CRC Press. doi:10.1201/b16912-5
- Schmitt, M. N., & Vihul, L. (Eds.). (2017). *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. doi:10.1017/9781316822524
- Speer, D. L. (2000). Redefining borders: The challenges to cybercrime. *Crime, Law, and Social Change*, 34(3), 259–273. doi:10.1023/A:1008332132218

Straub, D. W., & Collins, R. W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *Management Information Systems Quarterly*, 14(2), 143–156. doi:10.2307/248772

United States Bureau of Labor Statistics. (2018). Information security analysts job outlook. *Occupational Outlook Handbook*. Retrieved from <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>

Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information.*, 6(2), 183–211. doi:10.3390/info6020183

Wu, T. (2018). Is the First Amendment obsolete? *Michigan Law Review*, 117(3), 547–581.

ADDITIONAL READING

Bauman, Z. (1993). *Postmodern ethics*. Cambridge, UK: Polity Press.

Bossler, A. M., & Burruss, G. W. (2011). *The general theory of crime and computer hacking: Low self-control hackers? Corporate hacking and technology-driven crime: Social dynamics and implications* (T. J. Holt & B. H. Schell, Eds.). IGI Global.

Center for Strategic and International Studies. (2013) Report: The economic impact of cybercrime and cyberespionage. July. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

De Silva, E. (Ed.). (2016). *National Security and Counterintelligence in the Era of Cyber Espionage*. IGI Global. doi:10.4018/978-1-4666-9661-7

Dipert, R. R. (2010). Ethics of cyberwarfare. *Journal of Military Ethics*, 9(4), 384–410. doi:10.1080/15027570.2010.536404

Javers, E. (2011) Secrets and lies: The rise of corporate espionage in a global economy. *Georgetown Journal of International Affairs*, 12(1), 53-60.

Rishikof, H., & Lunday, K. (2011). Corporate responsibility in cybersecurity: Building international global standards. *Georgetown Journal of International Affairs.*, 12(1), 17–24.

United States Department of Justice. (2015) Prosecuting computer crimes: Computer crime and intellectual property section, Criminal Division. Office of Legal Education, Executive Office for United States Attorneys. Retrieved from <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>

Grey Zone Conflicts in Cyber Domain: Nonlocality of Political Reality in the World of “Hyperobjects”

2

Muhammed Can

University of Minho, Portugal

INTRODUCTION

Living in the age of advanced technologies comes with a price: Witnessing exponential growth in artificial intelligence, software-hardware systems and the cyber domain has rendered problems more ambiguous. The vulnerabilities of states, societies and individuals have become more evident thanks to the advent of these technologies. One of the most challenging manifestations can be seen in the grey zone conflicts which state and non-state actors constantly mobilize in order to show their strength. Given the existence of weapons of mass destruction (WMD) and deterrence among great powers, it is roughly impossible to expect great powers to dare overt sabre-rattling, which would eventually lead to total chaos throughout the world. Therefore, grey zone conflicts or political warfare has become both a lesser evil and low-cost option for rival states. As Mazarr puts it, grey zone conflicts consist of “salami-slicing strategies, fortified with a range of emerging area or unconventional techniques from cyberattacks to information campaigns to energy diplomacy” (2015, p.2).

Russia’s influence operations and alleged interference in the US elections in 2016, Chinese efforts to shift status quo in the South China Sea, Iran’s way of using grey zone tactics via proxies in its immediate vicinity and the pervasive utilization of unconventional tactics by terrorist organizations, notably by the so-called ‘ISIS’, make grey zone conflicts more significant not only for states but also for laypeople, whose lives are affected by these conflicts along a spectrum of severity. These impacts can be easily discerned in the election process, the perception of reality, diplomatic bargains, unexpected interference by major powers (annexation of Crimea through ‘little green men’) and information warfare.

It is evident that the cyber domain is a major part of grey zone conflicts. Cyberattacks on the political campaign of Emmanuel Macron, the Russian-backed hackers Cozy Bear and their ‘Lisa case’ attacks in Germany, the cyber conflict between Russia and Estonia, and Russian influence campaigns in Sweden, Ukraine and Georgia are among the most recent examples of grey zone conflicts in the cyber domain. In the same vein, it is also explicit that these confrontations between rival states have impacted the nature of political realities, which have rendered merely ‘virtual’ the function of conventional democratic practices – particularly in authoritarian regimes – just as occurred in the post-Soviet landscape (Wilson, 2005).

Apart from being in the midst of these conflicts, political realities have become more ambiguous, which adversely affects states, non-state groups and societies. Moreover, these political realities that are particularly manufactured in the cyber domain have become a nonlocal ‘hyperobject’, which simply refers to “genuine nonhuman objects that are not simply the products of a human gaze” (Morton, 2015, p.199). In his seminal book, Morton coined the term ‘hyperobject’ via object-oriented ontology. For

him, hyperobjects represent the coexistence of humans and objects and simply correspond to “things that are massively distributed in time and space relative to humans” (Morton, 2015, p.1). Therefore, a hyperobject might be the biosphere, a black hole, uranium or plutonium, or it might be “the very long-lasting product of direct human manufacture”, all of which have a plethora of features in common (Ibid). Firstly, hyperobjects are vicious, meaning that “they stick to beings that are involved with them” (Ibid). Secondly, hyperobjects pervade high-dimensional space, and their effects can be found ‘interobjectively’ in a space that includes interdependence between the “aesthetic properties of objects”. Finally, they are nonlocal, meaning that “they involve profoundly different temporalities than the human-scale ones we are used to” (Ibid).

Therefore, this chapter primarily seeks to reach possible answers regarding how the cyber domain of grey zone conflicts affects the political realities on the frontlines. It also attempts to reach an appropriate conclusion to determine possible regulations and existing conventions to counter grey zone conflicts in the cyber domain. Finally, it investigates the reality itself – and its manipulative nature – by putting ‘hyperobjectivity’ at the centre in the context of political reality.

MODERN GREY ZONE CONFLICTS IN THE CYBER DOMAIN

Grey zone confrontations are not a new phenomenon; they are “a nuanced form of warfare where antagonists seek limited political victories, as opposed to outright military triumphs that would be easier to identify and respond to” (Matissek, 2017, p.2). What makes these types of conflicts problematic is that they technically occur between the lines of peace and war, which is not in accordance with NATO’s Article 5 threshold or the UN Security Council’s definition of violence of (Echevarria, 2016). In the wake of World War II, major powers have started to use limited force to eschew total disaster. This type of conflict usually comprises diplomatic, information/cyber, military and economic areas (DIME) “to gain influence and leverage or weaken, destabilize, subvert or overthrow governments without resorting to war” (Robinson et al., 2018, p.8).

Grey zone conflicts “have been conducted in the past under such name as ‘political warfare’, ‘covert operations’, ‘irregular or guerrilla warfare’, ‘active measures’ and the like” (ISAB report, 2017, p.1). The term ‘political warfare’ can be traced back to 1948, when it was coined by American diplomat George Kennan in a memorandum. He defines it as “the logical application of Clausewitz’s doctrine in time of peace.” In the broadest definition, political warfare/grey zone conflicts are the employment of all the means at a nation’s command, short of war, to achieve its national objectives. Such operations range from overt actions such as political alliances, economic measures (like ERP – the Marshall Plan) and “white” propaganda to covert operations such as clandestine support of “friendly” foreign elements, “black” psychological warfare and even encouragement of underground resistance in hostile states“(Robertson et al., 2018, p.2). Furthermore, according to the United States Army Special Operations Command (2018, p.2), “political warfare/grey zone conflicts encompasses a spectrum of activities associated with diplomatic and economic engagement, Security Sector Assistance (SSA), novel forms of Unconventional Warfare (UW), and Information and Influence Activities (IIA)”.

Keeping that in mind, the characteristic of grey zone conflicts might include (ISAB report, 2017, p.2):

- Cyber, information operations, efforts to undermine public/allied/local/regional resistance, and information/propaganda in support of other hybrid instruments;
- Covert operations under state control, espionage, infiltration, and subversion;

- Special Operations Forces (SOF) and other state-controlled armed units, and unacknowledged military personnel;
- Support logistical, political, and financial – for insurgent and terrorist movements;
- Enlistment of non-governmental actors, including organized criminal groups, terrorists, and extremist political, religious, and ethnic or sectarian organizations;
- Assistance to irregular military and paramilitary forces;
- Economic pressures that go beyond normal economic competition;
- Manipulation and discrediting of democratic institutions, including the electoral system and the judiciary;
- Calculated ambiguity, use of covert/unacknowledged operations, deception and denial; and
- Explicit or implicit threat use, or threats of use of armed force, terrorism, and abuse of civilian populations and of escalation.

The vast majority of existing studies in the literature examine grey zone conflicts by drawing particular attention to the Cold War (Linebarger, 1948; Lord and Barnett, 1989; Goldstein and Finley, 1996; Pitney, 2001). However, particularly in the wake of the Cold War, most conflicts have become limited and hybrid in their nature due to the increasing costs of keeping boots on the ground (Fish et al., 2004; Smith Jr, 1989; Waltz, 1998). Therefore, the evolving nature of conflict has enabled relatively weaker actors to engage in information warfare, subversion techniques, and the cyber domain of grey zone conflicts (Mazarr, 2015; Schwartz, 2015; Macdonald, 2006).

Perhaps one of the most sophisticated ones is the Russian way of taking “active measures” in grey zones (Darczewska and Zochowski, 2017). As Polyakova and Boyer put it, “the Kremlin’s ‘active measures’ – covert activities aimed at influencing politics, narratives, and policies in favour of Russia’s geopolitical interests – evolved from overt to covert, physical to digital, conventional to asymmetric. The new tools are cheaper, faster and allow for maximum plausible deniability” (2018, p.2).

Apart from Russia, China has also used different tools that are categorized as unconventional means by coining ‘three warfares’ and ‘unrestricted warfare’ under the command of the People’s Liberation Army’s General Political Department to respond to possible challenges in grey zones (Liang and Xiangsu, 1999; Halper, 2013; Stokes and Hsiao, 2013). Furthermore, rogue states and other non-state groups pervasively exploit these power vacuums to compete with political rivals in different regions. For instance, Iran has recently been using ‘action networks’ by “implementing the covert elements of Iran’s foreign policy agenda, from terrorism, political, economic and social subversion; to illicit finance, weapons and narcotics trafficking; and nuclear procurement and proliferation” (Modell and Asher, 2013, p.8).

In the same vein, the most puzzling area of grey zone confrontations is the cyber domain, which might entail unexpected political and societal consequences at the global level. States opt for grey zone conflicts in the cyber domain partly because of their desire to shape perceptions to gain credibility and support for the legitimacy of their political objectives (Forest, 2009). These strategic moves consist of different ‘active measures’ including information warfare, psychological operations, public diplomacy and strategic communication (August, 2016). Russia is arguably the most sophisticated state, with a huge capacity to alter perceptions in different domains through its active measures. According to the US Senate’s Select Committee on Intelligence, “in the past 60 years, active measures became the norm; in the past 20 years, aggressive Russian digital espionage campaigns became the norm too” and finally “in the past 2 years, Russian intelligence operators began to combine the two – hacking and leaking – or digital espionage and active measures” (Rid, 2017).

Russia's strategy to exploit the information landscape includes a wide range of tactics. Ajir and Vailant (2018, p.77) classify these as follows:

- *Direct lies for the purpose of disinformation both of the domestic population and foreign societies;*
- *Concealing critically important information;*
- *Burying valuable information in a mass of information dross;*
- *Simplification, confirmation, and repetition (calculation);*
- *Terminological substitution: use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events;*
- *Introducing taboos on specific forms of information or categories of the news;*
- *Image recognition: known politicians or celebrities can take part in political actions to order, thus exerting influence on the worldview of their followers;*
- *Providing negative information, which is more readily accepted by the audience than positive.*

REVIVAL OF RUSSIAN ACTIVE MEASURES THROUGH CYBERATTACKS AND CHINESE CASE

In 2007, Estonia was hit by unexpected cyberattacks that took down the online services of media outlets, banks and other government facilities (McGuinness, 2017). Unprecedented waves of spam were sent by botnets, and automated online requests swamped servers, which eventually blocked cash machines, disabled communication among government employees and caused news outlets' news-delivery information flows to malfunction (Ibid). The underlying reason behind the attacks was Tallinn's decision to remove a Soviet World War II memorial – which was dubbed the 'bronze soldier incident' – which sparked outrage in the Russian government (Tamkin, 2017).

However, that was not the last Russian cyberattack. A year later, during the invasion of Georgia, it simultaneously conducted cyber action and a military operation by shutting down Georgia's internal communications (Windrem, 2016). The very fact that Georgia is a former Soviet country doubled the Kremlin's sensitivity whilst conducting strategic 'active measures'. Another Soviet successor state, Kyrgyzstan, was attacked by Russian hackers through distributed denial of service (DDoS) in 2009 (Ibid). It initially aimed at shutting down two of the country's four internet service providers (Ibid). However, the strategic point was Russia's demand for the eviction of a US military base, which Kyrgyzstan eventually met in return for \$2 billion in aid from Moscow.

A DDoS was also evident in the grey zone confrontation with Estonia in 2007. As Valeriano and Maness suggest, "these operations flood particular Internet sites, servers, or routers with more requests for data than the site can respond to or process", which eventually "shuts down the site, thereby preventing access or usage (2015, p.34). Apart from that, Structured Query Language (SQL) injection was commonly used by Russian hackers – particularly in the Georgian War in 2008 – to alter the status quo in different contested regions (Carr, 2012). This type of attack "takes over the site for a few hours or days and displays text or pictures that demean or offend the victim site" (Valeriano and Maness, 2015, p.34). Through the SQL injection, the attacker might execute random SQL queries on the backend database server, which is a highly critical application issue, resulting in the loss of all the data stored (Carr, 2012).

Intrusions, which include Trojans and trapdoors, are another major tool in grey zone conflicts to subvert rivals' strategic agendas. They are more targeted, consisting of "unauthorised software added to a program to allow entry into a victim's network or software program" (Valeriano and Maness, 2015, p.34). The Chinese gh0st remote access tool (RAT) – a type of Trojan – is perhaps one of the most significant of them. It was used as a part of cyber espionage attempt by Chinese hackers which affected 1300 computers in 103 countries, including government bodies, media outlets and nongovernmental organisations (Carr, 2012). Speaking of the effects of these attacks in politics – particularly as a grey zone activity – the latest French election would be a proper example, even though there was no compelling evidence whether attacks impacted the election results.

It is commonly known that this type of interventions in the cyber domain is highly related to the situation of 'plausible deniability', which potentially eases the burden of the aggressor state. It might be a part of a specific special operation, a psychological operation (PSYOP) – which directly aims at altering the perception of the target audience (TA), whether it be in war or not – or political warfare in grey zones. It is also significant to stress that the Russian parlance of cyber warfare does not correspond to the conventional definition; rather, it covers computer network operations, electronic warfare, psychological operations and information operations (Connell and Vogler, 2017).

The 'Macron leaks' incident was an explicit instance that entails a huge controversy among post-Cold War rival states. Hours before the election, Emmanuel Macron's political campaign was targeted and attacked by unknown proxies who revealed thousands of Macron's campaign team's emails (Willsher and Henley, 2017). It turned out later that behind the attack was a Russian hacking team, the so-called 'Advanced Persistent Threat 28' (APT 28), 'Fancy Bear' or 'Pawn Storm', who allegedly have a direct link to the Russian military intelligence directorate (GRU) (Hern, 2017). The method used in the Macron Leaks incident was 'spear phishing', which creates fake login pages to entice targeted individuals to enter their usernames and passwords, giving the hackers unlimited access to their confidential information (Ibid).

However, some argue that spear phishing is not a sophisticated method, even though it has successfully impacted high-profile networks (Valeriano and Maness, 2015). Be that as it may, the political reality and its serious consequences are at stake when it comes to considering whether a cyberattack is successful or not in grey zones. For instance, the Russian cyberattack to alter the Ukrainian election result was a direct attempt to change the political reality on the ground. Russian-linked hackers attacked Ukraine's central election commission, deleted key files and implanted a virus in order to change the result of an election in favour of a Russian-backed party (Polyakova and Boyer, 2018). However, one hour before the announcement of the election result, these attacks were detected by Ukrainian security officers (Ibid). Although Ukrainian officials kept these crisis moments under control, Russian media outlets still wittingly reported the fake results, showing the Russian-backed party winning despite the fact that it just had 1 per cent of total votes (Ibid).

Having mentioned that, Russian information operations in grey zones are not limited to cyberattacks. They also frequently use social media and other conventional broadcasting methods. One of the recent examples is the 'Lisa case', which abruptly affected the perception of mobs in Germany in 2016. It was alleged by the media that a German girl with a Russian origin had been raped by several migrants in Berlin, which prompted far-right groups to march against migrants (Janda, 2016). However, in the wake of the tumultuous protests, a teenage girl admitted that she had made up the story of alleged rape by migrants (Knight, 2016).

In the social media landscape of grey zone conflicts, Russia has constantly staged malicious information operations. The most prominent and recent one is the alleged intervention in US elections in 2016. As the US Office of the Director of National Intelligence assessment claims, Russian influence campaign

encompassed a “messaging strategy that blends covert intelligence operations – such as cyber activity – with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and social users or trolls” (2017, p.2). In addition to this, Russia dexterously controlled the narratives regarding the downing of Malaysia Airlines Flight 17 and its poisoning of its former spy Sergei Skripal through social media (Bodine-Baron et al., 2018).

It is an unequivocal fact that Russian activities in the grey zone are not a new phenomenon. On the contrary, they trace back to the Cold War period. As the US Department of State pointed out, in 1985, the Soviet Union started a campaign in order to alter perceptions by spreading fake news that claimed the “AIDS virus had been manufactured as a result of genetic engineering experiments conducted at Fort Detrick, Maryland, allegedly to develop new biological weapons” (1987, p.33). What is more bizarre is another report from this period by the US Information Agency which suggested that Russian media had been constantly circulating an accusation that the United States was conducting covert scientific research to develop an ‘ethnic weapon’ that would be able to kill only non-whites (1988).

In the same vein, the Chinese way of pursuing operations in grey zones – particularly in the cyber and information domain – is similar to Russia’s. Chinese strategic thinking with regard to operating in grey zones also traces back to the Cold War period, apart from the fact that its grand strategy hinges upon the tenets of Sun Tzu. At the end of the 1990s, two Chinese military officers coined the term ‘unrestricted warfare’, emphasising the evolving character of warfare (Liang and Xiangsui, 1999). In subsequent years, the Chinese Communist Party, Central Committee and Central Military Commission ratified the concept of ‘three warfares’ that comprise following three major areas: psychological warfare, media warfare and legal warfare (Halper, 2013).

Particularly in the cyber domain of grey zone conflicts, China has allegedly been involved in different attacks. The most critical example was a Chinese attack on US nuclear weapons laboratories in 2007, when attackers made roughly 1,100 attempts to steal data through different strategies, including sending phishing e-mails to staff (Markoff, 2007). And the United States was not alone in being targeted by China: The United Kingdom and its business sector were also at the epicentre of these attacks. According to a 2008 report of the UK’s domestic security service (MI5), Chinese intelligence agencies have constantly attempted a wide range of attacks to hack the computers of British companies in order to blackmail prominent businesspeople over their improprieties (Burns, 2010). In the following year, the UK’s domestic and foreign security agencies suggested that China’s illegal cyber activities in grey zones had become extremely sophisticated, potentially enabling attackers to shut down several infrastructures comprising food, power and water supplies (Hjortdal, 2011).

China is not only using its cyber capability to compete with its ‘archenemies’ but also for its long-term strategic goals, predominantly in the immediate vicinity. Over the past several years, it has attacked Taiwanese government computers, reaching almost 10 million attacks a month (Yu, 2018). Without any doubt, this is a part of Chinese grey zone strategy that directly relates to its protracted territorial disputes. However, some argue that the underlying reason for these attacks in grey zones is China’s desire to outperform the US in the cyber domain while avoiding being looked at as a malicious actor (Starks, 2018).

Contests in the grey zones – diplomatic, informational/cyber, military and economic – are directly related to the intervening status quo of a balance of power or threat. However, how to deal with the legal status of this type of conflict, especially in the cyber domain, remains the million-dollar question. Indeed, how might authorities conceptualise cyberattacks in grey zones? Should they be regarded as state crimes? Which legal framework would be proper to avoid harmful consequences from this type of conflict?

The Legal Status of Grey Zone Activities in the Cyber Domain: The *Jus ad Bellum* and *Jus in Bello* Dilemma

The problem of how to deal with these attacks in the legal framework is highly tricky given the complexity of the nature of grey zone conflicts. These grey areas are not the only thing that creates ambiguity – determining perpetrators within the legal boundaries is extremely challenging. Brooks draws attention to this point by remarking, “We struggle to tell the difference between civilians and combatants. What counts as a protected civilian object in cyberspace? When can a hacker, a financier, or a propagandist be considered a combatant? When, if ever, is it lawful for a state to respond to a non-kinetic attack using conventional military force?” (2018, para.7).

Perhaps the first step toward reaching a legal way out lies behind two legal principles. International law determines two ways to look at wars. The first is *jus ad bellum* – which accounts for ‘justice to war’ – whose legal source stems from the Charter of the United Nations in Article 2 and Article 51, which states, “all members shall refrain in their international relations from the threat or the use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations”, and “nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations” (1945).

The second one is *jus in bello*, which accounts for ‘justice in war’ and “governs the conduct of war once it has started” (Greenwood, 1983, p.221). This subdivision of law hinges upon customary law and treaty laws – for instance, the Hague Regulations of 1899 and 1907 and the Geneva Conventions – to adjust the ethics of war. These two concepts are a major part of the Law of Armed Conflict (LOAC), which governs the conduct of armed conflict.

However, it is not certain which concept would be proper to apply to the cyber domain of grey zone conflict simply because of its pending definition. Furthermore, determining at which point in the escalation between rivals these conflicts ought to be accepted as war is still challenging. Even if rivals accept these activities as sabre-rattling or a declaration of overt war, it is still unclear which regulations would leverage the parties’ strategic position. It is also argued in the NATO Cooperative Cyber Defence Centre of Excellence’s manual – also known as the Tallinn Manual – that determining the threshold of cyberattacks in legal terms is highly complicated given the different strategies and considerations of states, including “views on the subject range from a full application of the law of armed conflict, along the lines of the International Court of Justice’s pronouncement that it applies to ‘any use of force, regardless of the weapons employed’, to strict application of the Permanent Court of International Justice’s pronouncement that acts not forbidden in international law are generally permitted” (Schmitt, 2013, p.3).

There are two main competing understandings regarding the possible legal framework for cyber conflicts. Russia supports an international treaty in compliance with the negotiated terms of chemical weapons, whilst the US finds an international treaty unnecessary (Markoff and Kramer, 2009). According to a declaration issued by the White House, “the development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behaviour – in times of peace and conflict – also apply in cyberspace” (Schmitt, 2013, p.3).

Nevertheless, it is obvious that an international cyber treaty – which would directly impact the cyber frontier of grey zone conflicts – is inevitable given the exponential growth in technology. It is also evident that “the great powers will have no good choice but to cooperate and create rules, norms, and standards of behaviour to buttress what will essentially be a new political order” (Forsyth Jr. and Pope, 2014, p.112).

Another significant view is Shackelford's (2009) taxonomy of possible applicable legal frameworks as follows:

- The Antarctic Treaty System and Space Law
- Mutual Legal Assistance Treaties (MLAT)
- Nuclear non-proliferation treaties
- United Nations Convention on the Law of the Sea

Even if these suggested frameworks will be implemented in cyberspace in the near future, there are a wide range of thorny definitions that remain vague in the cyber frontier of grey zone conflicts. For instance, how should we define a breach of state sovereignty during state-backed attacks? Should these attacks be counted as direct intervention, just like physical ones? Possible answers represent different views with respect to the problem of sovereignty. Rule 4-1 of the Tallinn Manual 2.0 suggests that “cyber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law” (2017, p.17).

In this Manual, a majority of experts reached the conclusion that regardless of considering the physical damage – such as non-temporary loss of functionality of infrastructure – brazen cyberattacks by states targeting any country should be treated as violations of state sovereignty (Schmitt, 2017). In the same vein, “the rule of non-intervention is a natural derivative of the concept of sovereignty; to the extent that a State enjoys exclusive sovereign rights, other States necessarily shoulder a duty to respect them” (Ibid, p.7). However, this prohibition of non-intervention could be applied to the issues that fall into the *domaine réservé* of other states (Ibid). For instance, cyberattacks that target the results of elections must be regarded as interventions simply because they directly hinge upon the *domaine réservé*, while others – namely, attacks targeting business sectors in order to leverage vulnerabilities and secrets – cannot be assessed as interventions according to international law (Ibid). It is obvious that this line of reasoning is open to exploitation by aggressor states. By the same token, given the interwoven relations between state-related matters and other sectors, it might be naïve to assess cyberattacks in a different context by only focusing on the *domaine réservé*.

Having discussed the ways to tackle grey zone activities in the cyber domain through existing laws and regulations, it is now necessary to explain how these conflicts have the potential to shift political realities on the ground through the lens of ‘hyperobjectivity’.

Nonlocality of Hyperobjects and Political Realities

The post-truth, fake news, deep fakes, the populist rhetoric of far-right politicians, the propagandist agendas of authoritarian leaders and rising discrimination at the international level based on ethnicity, religion and sexual orientation are chronic problems of the post-Cold War world. But as Mark Twain's popular maxim puts it, “History doesn't repeat itself, but it often rhymes,” so it is almost certain that these aforementioned trends are not new (Cowie, 2009). Rather, the most challenging issue facing the world facing might be the complex relationship between technology and politics. It is possible to witness a more multifaceted interdependency in the near future given the recent unprecedented advancements in artificial intelligence (AI), deep learning and computer systems. Perhaps it will turn into a common principle that ‘who controls technology, engineers reality’, which might render politics purely virtual under the control of ‘political technologists’ (Wilson, 2005).

The construction of political reality has been one of the most contested concepts over the decades. In his seminal article, Edelman argues that “the critical element in a political manoeuvre for advantage is the creation of meaning: the construction of beliefs about the significance of events, of problems, of crises, of policy changes, and of leaders. The strategic need is to immobilize opposition and mobilize support” (1985, p.10). Creation of meaning directly depends on the capability of states and non-state actors to represent realities. Regardless of the ethics and reliability of these realities, political actors might leverage in favour of their political agenda, particularly if the balance of power/threat is at stake.

Beyond that, the use of language and symbols is highly significant in altering the nature of political realities (Burnier, 1994). In grey zone conflicts, states have an immense capability to intervene in the nature of reality through the control of information flow, information operations (IO) and psychological operations (PSYOPs).

Therefore, cyberspace is the most susceptible part of these conflicts due to the lack of international norms and rules. Perhaps the most significant point is the ontological problem of how these realities might alter perceptions at the global level. They have surpassed being objects; rather, they have turned into hyperobjects that might ramble on anywhere in the world thanks to the power of cyberspace. Timothy Morton is the first scholar who coined the term ‘hyperobjects’ within the context of object-oriented ontology. He defines “hyperobjects to refer to things that are massively distributed in time and space relative to humans. A hyperobject could be a black hole. A hyperobject could be the Lago Agrio oil field in Ecuador or the Florida Everglades. A hyperobject could be the biosphere or the Solar System. A hyperobject could be the sum total of all the nuclear materials on Earth; or just the plutonium, or the uranium” (2013, p.1). For him, hyperobjects are the product of the current age of asymmetry between humans and nonhumans (Ibid, p.161).

Moreover, the effects of hyperobjects are worldwide, just like those of global warming, even if they cannot be perceived in tangible forms (Ibid). The main problem regarding hyperobjects, however, is, “how can we know it is real? What does it really mean? The threat of global warming is not only political but also ontological. The threat of unreality is the very sign of reality itself. Like a nightmare that brings news of some real psychic intensity, the shadow of the hyperobject announces the existence of the hyperobject” (Ibid, p.32). The reality, therefore, becomes a nonlocal hyperobject (to borrow an analogy from quantum theoretical psychics that refers to the ostensible ability of objects to directly know each other’s states, even when physically disconnected from each other) in line with the exponential growth in technology.

This argument is valid for the grey zone conflicts in cyberspace. Firstly, even if they do not have physical embodiment, their impacts – particularly with respect to the nature of reality – could cause a global tragedy. The aforementioned ‘Lisa case’ and the alleged Russian cyber intervention in the latest French, American and Ukrainian election were about shifting the political reality, along with the attacks on Estonia and Georgia, even though their effects remained limited. In addition, Chinese cyberattacks on Taiwan, the US and other rival countries were also aimed at intervening in the political reality.

Secondly, the asymmetric nature of grey zone conflicts in cyberspace is similar to the proposed features of hyperobjects, which might appear in the guise of post-truth, fake news and deep fakes throughout the world in a different context.

Finally, these attacks have an immense potential to spread unrealities – in the same way that the diffusion of nonlocal subatomic particles does – even though the differences between the contexts of cases might entail various consequences.

Therefore, political realities/unrealities no longer depend only on the use of language or symbols in political rhetoric in this asymmetric age of politics and related issues. Therefore, cyberspace constitutes the most significant frontier for both states and non-state actors to eliminate their status quo in line with their strategic agendas.

Various solutions can be employed to the cyber domain of grey zone conflicts to overcome the dissemination of political unrealities/realities as follows:

- Agreed international regulations are the most significant prerequisite for reaching a more secure environment in the cyber-domain.
- The definition of cyberattacks ought to be completed through the consensus of competing parties in different landscapes.
- Defining which activities are considered as violations of sovereignty under the umbrella of intervention in the cyber domain is highly significant given the tenuous application of *domaine réservé*.
- Information flow must be controlled based on existing laws by detecting malicious accounts and activities.
- There is also a particular need to establish an international organisation to prevent state-backed cyberattacks by identifying perpetrator states.
- To counter disinformation campaigns in grey zones – in both social media and conventional media – the truth should be revealed as soon as possible to limit the disinformation's diffusion and shift the disadvantageous position of targeted states.
- It is also important to note that limiting and discouraging attacks/activities of authoritarian states in grey zones requires reifying a grand strategy, similar to what was stated in the third-offset strategy of the US (Centre for Strategic and International Studies, 2017).
- Apart from deterrent measures – imposing economic sanctions, suspending multilateral diplomatic talks, military drills or pressures coming from International Organisations – the targeted countries should employ offensive tactics and strategies to counter these attacks.
- Improved defensive firewalls – in conjunction with the recent developments in AI, deep learning, software and hardware systems – are another aspect of the cyberspace frontier of grey zone conflicts, as they have been constantly exposed to ATPs, phishing attacks, Trojan horses and backdoors.
- Governments and international institutions should be informed and up to date with respect to possible future attacks and the nature of attacks in grey zones along with the historical aspects of grey zone conflicts.

Further research needs to examine more closely how cyberattacks would impact other frontiers of grey zone conflicts. For instance, to what extent can cyberattacks alter conflicts in other landscapes, such as the economic, diplomatic, military and intelligence domains? Current understanding of grey zone conflicts is too premature to identify the interwoven relations among such domains, although there is a large body of literature with respect to the current strategies of China, Russia, Iran, North Korea and non-state actors. Therefore, further study could compare the long- and short-term effects of these conflicts. It is also significant to note that there is no exact scientific taxonomy regarding grey zone conflicts. Thus, future studies may classify grey zone conflicts – particularly conflicts in cyberspace – in order to determine how existing rules might be applied to a given case.

CONCLUSION

Returning to the question posed at the beginning of this chapter, it is now possible to state that the unregulated cyber domain of grey zone conflicts is highly challenging for democratic countries, considering that their counterstrategies are restricted by domestic laws. Perhaps Russia is the most capable country in grey zones – in different domains – given the fact that it has engaged in constant interventions since the communist revolution took place. The latest activities in Ukraine were unexpected and unusual for Western countries. China is the second country that continues to operate in different landscapes in line with its grand strategy. Iran, North Korea and non-state actors are also major players in these conflicts.

Furthermore, it has been proved that grey zone conflicts will remain a primary tool for rival countries to help sustain conflicts below the threshold of war. They are also cheaper and less risky, so rival countries might pay a lower price compared with the catastrophic consequences of total war. Having said that, there is no certain explanation as to whether grey zone activities in cyberspace should be treated as state crimes, acts of war, interventions or violations of sovereignty. What is more problematic are the effects of these cyberattacks on the political realities/unrealities. Needless to say, these unrealities have become nonlocal hyperobjects that spread instantly anywhere in the world, regardless of the context. Even though it is not possible to see the immediate consequences of these conflicts in the cyber domain, it will be more challenging for countries unless global cooperation will be established through the regulations.

REFERENCES

- Ajir, M., & Vaillant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70–89.
- August, M. B. (2016). *The Red Zone: Russian conflict management in the Gray Zone* (Doctoral dissertation, Sciences).
- Bodine-Baron, E., Helmus, T., Radin, A., & Treyger, E. (2018). *Countering Russian Social Media Influence*. RAND Cooperation. Retrieved from https://www.rand.org/pubs/research_reports/RR2740.html
- Brooks, R. (2018). *Rule of Law in the Gray Zone*. Retrieved from <https://mwi.usma.edu/rule-law-gray-zone/>
- Burnier, D. (1994). Constructing political reality: Language, symbols, and meaning in politics: A review essay. *Political Research Quarterly*, 47(1), 239–253.
- Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc.
- Center for Strategic and International Studies. (2017). Assessing the Third Offset Strategy. *CSIS*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170302_Ellman_ThirdOffsetStrategy-Summary_Web.pdf?EXO1GwjFU22_Bkd5A.nx.fJXTKRDKbVR
- Charter of the United Nations. (1945). Retrieved from <http://www.un.org/en/sections/un-charter/un-charter-full-text/>
- Connell, M., & Vogler, S. (2017). *Russia's approach to cyber warfare*. Center for Naval Analyses Arlington United States.

Cowie, I. (2009). *History does not repeat itself, but it often rhymes, as Mark Twain noted*. Retrieved from <https://www.telegraph.co.uk/finance/personalfinance/comment/iancowie/5018093/History-does-not-repeat-itself-but-it-often-rhymes-as-Mark-Twain-noted.html>

Darczewska, J., & Żochowski, P. (2017). Active Measures: Russia's Key Export. *OSW Studies*, 64.

Echevarria, A. I. (2016). *Operating in the gray zone: An alternative paradigm for US military strategy*. Army War College-Strategic Studies Institute Carlisle United States.

Edelman, M. (1985). Political language and political reality. *PS, Political Science & Politics*, 18(1), 10–19. doi:10.1017/S1049096500021247

Fish, J. M., Reddish, C. J., & McCraw, S. J. (2004). *Fighting in the gray zone: a strategy to close the preemption gap*. DIANE Publishing.

Forest, J. J. (2009). *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas*. ABC-CLIO.

Forsyth, J. W. Jr, & Pope, B. E. (2014). Structural causes and cyber effects: Why international order is inevitable in cyberspace. *Strategic Studies Quarterly*, 8(4), 112–128.

Goldstein, F. L., & Findley, B. F. (1996). *Psychological Operations: Principles and case studies*. Air Univ Maxwell AFB AL.

Greenwood, C. (1983). The Relationship between ius ad bellum and ius in bello. *Review of International Studies*, 9(4), 221–234. doi:10.1017/S0260210500115943

Halper, S. (2013). China: The three warfares. Report for the Office of Net Assessment, US Department of Defense.

Hern, A. (2017). *Macron hackers linked to Russian-affiliated group behind US attack*. Retrieved from <https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack>

Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Security*, 4(2), 2. doi:10.5038/1944-0472.4.2.1

ISAB. (2017). *Report on Gray Zone Conflict*. Retrieved from <https://www.state.gov/t/avc/isab/266650.html>

Janda, J. (2016). *The Lisa Case STRATCOM Lessons for European states*. Federal Academy for Security Policy Working Paper No.11/2016.

Knight, B. (2016). *Teenage girl admits making up migrant rape claim that outraged Germany*. Retrieved from <https://www.theguardian.com/world/2016/jan/31/teenage-girl-made-up-migrant-claim-that-caused-uproar-in-germany>

Liang, Q., & Xiangsui, W. (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House Arts.

Linebarger, P. M. (1948). *Psychological warfare*. Pickle Partners Publishing.

Lord, C., & Barnett, F. (Eds.). (1989). *Political Warfare and Psychological Operations: Rethinking the US Approach*. DIANE Publishing.

Macdonald, S. (2006). *Propaganda and Information Warfare in the Twenty-First Century: Altered images and deception operations*. Routledge. doi:10.4324/9780203967393

Markoff, J. (2007). *Cyber attack on U.S. nuclear arms lab linked to China*. Retrieved from <https://www.nytimes.com/2007/12/09/world/americas/09iht-hack.1.8653712.html>

Markoff, J., & Kramer, A. (2009). *U.S. and Russia Differ on a Treaty for Cyberspace*. Retrieved from <https://www.nytimes.com/2009/06/28/world/28cyber.html?mtrref=www.google.com.tr>

Matissek, J. W. (2017). Shades of Gray Deterrence: Issues of Fighting in the Gray Zone. *Journal of Strategic Security*, 10(3), 2. doi:10.5038/1944-0472.10.3.1589

Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. US Army War College Strategic Studies Institute Carlisle.

McGuinness, D. (2017). *How a cyber attack transformed Estonia*. Retrieved from <https://www.bbc.com/news/39655415>

Modell, S., & Asher, D. L. (2013). *Pushback: Countering the Iran Action Network*. Center for a New American Security.

Morton, T. (2015). *Hyperobjects: Philosophy and Ecology after the End of the World*. University of Minnesota Press.

Narula, S. (2004). Psychological operations (PSYOPs): A conceptual overview. *Strategic Analysis*, 28(1), 177–192. doi:10.1080/09700160408450124

Pitney, J. J. Jr. (2001). *The art of political warfare*. University of Oklahoma Press.

Polyakova, A., & Boyer, S. (2018). *The Future of Political Warfare: Russia, the West, and Coming Age of Global Digital Competition*. Brookings Institution. Retrieved from <https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf>

Rid, T. (2017). *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*. Select Committee on Intelligence, US Senate, 30.

Rid, T., & Hecker, M. (2009). *2.0: Irregular Warfare in the Information Age: Irregular Warfare in the Information Age*. War. ABC-CLIO.

Robinson, L., Helmus, T., Cohen, R., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2018). *Modern Political Warfare: Current Practices and Possible Responses*. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1772.html

Schleifer, R. (2014). *Psychological Warfare in the Arab-Israeli Conflict*. Springer. doi:10.1057/9781137467034

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. doi:10.1017/CBO9781139169288

- Schmitt, M. N. (2017). *Grey Zones in the International Law of Cyberspace*. Academic Press.
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. doi:10.1017/9781316822524
- Schwartz, L. (2015). *Political Warfare Against the Kremlin*. Palgrave Macmillan.
- Shackelford, S. J. (2009). From nuclear war to net war: Analogizing cyber attacks in international law. *Berkeley Journal of International Law*, 27, 192.
- Smith, P. A. Jr. (1989). *On political war*. National Defense Univ.
- Starks, T. (2018). Sizing up Chinese, North Korean cyberattacks. *Politico*. Retrieved from <https://www.politico.com/newsletters/morning-cybersecurity/2018/06/15/sizing-up-chinese-north-korean-cyberattacks-252481>
- Stokes, M., & Hsiao, R. (2013). *The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics*. Project 2049 Institute.
- Tamkin, E. (2017). 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? *Foreign Policy*. Retrieved from <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>
- United States Department of State. (1987). Soviet influence activities: a report on active measures and propaganda, 1986-87 (Vol. 9627). US Department of State.
- United States Information Agency. (1988). *Soviet Active Measures in the Era of Glasnost*. Retrieved from <http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20in%20the%20Era%20of%20Glasnot%20March%201988.pdf>
- USA Office of the Director of National Intelligence. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf
- Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press. doi:10.1093/acprof:oso/9780190204792.001.0001
- Waltz, E. L. (1998). *Information warfare principles and operations*. Artech House, Inc.
- Willsher, K., & Henley, J. (2017). *Emmanuel Macron's campaign hacked on eve of French election*. Retrieved from <https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election>
- Wilson, A. (2005). *Virtual politics: faking democracy in the post-Soviet world*. Yale University Press.
- Windrem, R. (2016). *Timeline: Ten Years of Russian Cyber Attacks on Other Nations*. Retrieved from <https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111>
- Yu, J. (2018). *Chinese cyber attacks on Taiwan government becoming harder to detect: source*. Retrieved from <https://www.reuters.com/article/us-taiwan-china-cybersecurity/chinese-cyberattacks-on-taiwan-government-becoming-harder-to-detect-source-idUSKBN1JB17L>

ADDITIONAL READING

- Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.
- Arquilla, J., & Borer, D. A. (Eds.). (2007). *Information strategy and warfare: A guide to theory and practice*. Routledge. doi:10.4324/9780203945636
- Dinniss, H. H. (2012). *Cyber warfare and the laws of war* (Vol. 92). Cambridge University Press. doi:10.1017/CBO9780511894527
- Hoffman, F. G. (2016). The contemporary spectrum of conflict: protracted, grey zone, ambiguous, and hybrid modes of war. The Heritage Foundation, 25-36.
- Lovelace, D. (2016). *Hybrid warfare and the grey zone threat* (Vol. 141). Oxford University Press.
- Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*. Newnes.
- Votel, J. L., Cleveland, C. T., Connett, C. T., & Irwin, W. (2016). Unconventional warfare in the gray zone. *Joint Forces Quarterly*, 80(1).
- Yannakogeorgos, P. A., & Lowther, A. B. (Eds.). (2013). *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. CRC Press.

KEY TERMS AND DEFINITIONS

Cyber Sovereignty: This is a phrase commonly used in the field of internet governance to define the will of states to exercise and sustain control over the Internet domain within their own borders, including political, economic, cultural and technological activities. However, it is not clear how to apply this sovereignty concept to current international relations and international laws.

Cyberwarfare: Cyberwarfare is an overt or covert action of states, non-state actors or state-backed attackers that includes various tactics and techniques, notably advanced persistent threats, phishing tactics, viruses like Stuxnet, botnets, Trojan horses, zombies, Metasploit, SQL attacks, Rootkit, Nessus, pharming, Wireshark and buffer overflows to target infrastructure, software systems, and governmental institutions of different parties.

Grey Zone Threats: These are the threats that comprise a full spectrum of means and tools used by aggressor states to subvert their rivals' plans and strategies. These kinds of threats are perceived as affordable, less risky and flexible by the aggressor states.

Information Operations: Information operations are the part of political warfare/grey zone conflicts that occur in an asymmetrical way via social and conventional media, state organisations and military means to weaken the morale and psychology of enemy states.

The Law of Armed Conflict: The Law of Armed Conflict (LOAC), also known as the International Humanitarian Law, is a body of international law which regulates the behaviours of actors during armed conflict by ordering balance between military necessity and humanity. It comprises the Geneva Conventions, Hague Conventions and customary laws. It also limits the targeted attacks of combating parties in order to protect civilians and avoid total disaster.

Object-Oriented Ontology: Object-oriented ontology (OOO) is a school of thought which argues that objects exist independently of human understanding and perception. The term was coined by the philosopher Graham Harman. It is also designated in the existing literature as ‘speculative realism’, which criticises the reductionism of Kantian philosophy.

Ontological Approach to Cyberspace: It basically assesses cyberspace as a metaphysical laboratory that combines art and philosophy of things, machines and different domains, although this philosophical approach is not new.

Developing Cyber Buffer Zones

2

Michael Robinson <https://orcid.org/0000-0002-4276-2359>*Airbus, UK***Kevin Jones***Airbus, UK***Helge Janicke***De Montfort University, UK***Leandros Maglaras** <https://orcid.org/0000-0001-5360-9782>*De Montfort University, UK*

INTRODUCTION

Cyberspace has become the latest domain of war (Robinson, Jones, & Janicke, 2015), where modern international actors aggressively pursue their national security and foreign policy goals (Martins, 2018). Much research has been focused upon this area, covering topics such as the ethics of cyberwarfare (Dipert, 2010), legal aspects (Baradaran & Habibi, 2017), how best to conduct military operations inside of cyberspace (Liles, Rogers, Dietz, & Larson, 2012) and how to organise and defend nations from cyber attack (Ruiz, 2017) (THIBER (The Cybersecurity Think Tank), 2013). Surveys of the literature show a vast range of additional topics, demonstrating that research interest into cyber warfare is lively and diverse (Robinson, Jones, & Janicke, 2015). Whilst it is clear that interest in cyber warfare is high, there has been less attention paid to its aftermath. What effects on societies persist after cyber warfare and do these effects stymie work to restore peace and security to conflict torn regions?

The field of cyber peacekeeping addresses these questions, looking at conflicts which contain cyber warfare through the lens of peacekeeping. In this chapter, we provide a background to cyber peacekeeping and survey existing literature. We then make a contribution to the field by developing the concept of a cyber buffer zone.

BACKGROUND

The concept of cyber peacekeeping can be traced back to an article by Cahill, Rozinov and Mule (2003). They noted that cyber warfare would likely have devastating effects well beyond the boundaries of the combatants and that some kind of peacekeeping capability in cyberspace would be needed (Cahill, Rozinov, & Mule, 2003). Some potential cyber peacekeeping activities were proposed, such as cyber

DOI: 10.4018/978-1-5225-9715-5.ch019

border management and monitoring/verification and their overall approach was to explore how existing peacekeeping doctrine could be mapped to cyber warfare. The topic did not receive any further attention for ten years until Kleffner and Dinniss (2013) reignited discussion. They drew attention to the convergence of two significant global trends: an increase in conflicts which involve a cyber component and the increasing deployment of complex peace operations. They noted that these trends made it natural to assume that peacekeepers will find themselves asked to keep the peace in environments where the peace is threatened by cyber incidents (Kleffner & Dinniss, 2013).

Akatyev and James (2015) contributed by proposing a cyber peacekeeping model, including a set of goals and proposals of activities to perform during three stages: no conflict, conflict and post-conflict. In the no conflict stage, cyber peacekeepers work to unite efforts to keep the peace and prevent the outbreak of cyber conflict. In the conflict stage efforts are directed to orchestrating an international response and containing the harmful effects (e.g. through preventing the spread of malware or cyber weapons). Finally in the post-conflict stage, they propose that cyber peacekeepers are tasked with preventing further destruction and recovering critical infrastructure back to operation. In this regard, the model covers all three phases of warfare with the primary goal of protecting civilians.

The need for cyber peacekeeping was reinforced two years later by Dorn (2017), who states that cyberpeacekeepers could patrol and act in cyberspace just as current UN peacekeepers patrol and act in the world's conflict zones. Faced with a huge disaster bill and a potential for vast escalation in attacks, an investment in cyberpeacekeeping would seem like a bargain (Dorn, 2017).

In 2018, Robinson et al. (2018) built upon the foundations set by Cahill, Rozinov and Mule back in 2003. They reinforced the need for cyber peacekeeping with specific cases where cyber warfare would present a threat to international peace and security as defined by the United Nations. They explored how the activities of a modern multi-dimensional peacekeeping operation could be translated into a cyber warfare context, and evaluated each one according to two core criteria: value and feasibility. Any activity performed during cyber peacekeeping must bring clear value towards restoring peace and security, and must also be feasible to perform. They conclude that many of the existing UN peacekeeping activities would bring value in a cyber warfare context, but that feasibility can vary due to technical and political constraints.

Whilst such research into cyber peacekeeping is gaining momentum, further work is needed to develop the proposed activities and ideas into something practical: actions that could be concretely performed by peacekeepers in a cyber context to tangibly promote peace. The aim of this article is to contribute towards this goal by focusing on the concept of buffer zones.

FOCUS OF THE ARTICLE

In this article, we build upon the work of Robinson et al. (2018) by taking a closer examination of just one of the proposed activities: cyber buffer zones. The aim is to propose how the traditional peacekeeping activity of creating and running a buffer zone could be translated into cyber terms. To achieve this goal, we begin with a brief background of traditional buffer zones as used by UN peacekeeping. We then propose how the concepts behind a buffer zone could be translated into cyber terms, with emphasis on practical feasibility and ensuring that any proposal brings value towards peace. Data for this translation comes from both the cyber security and peacekeeping domains.

For this work, we adopt the methodology of Design Science Research (DSR) (Vaishnavi & Kuechler, 2015). The DSR approach is a set of synthetic and analytical techniques and perspectives (complementing positivist, interpretive, and critical perspectives) for performing research. The approach is directed toward understanding and improving the search among potential components in order to construct an artifact that is intended to solve a problem (Baskerville, 2008). It encourages problem solving through an approach of innovative solution design, where the focus of the work is upon contributing interesting, new and true knowledge through novel designs. In a new field such as cyber peacekeeping, where there is little existing knowledge, the DSR methodology is an ideal approach. The first stage of the DSR process is an awareness of the problem.

AWARENESS OF THE PROBLEM

Authors such as Robinson et al. (2018) and Akatyev and James (2015) have made a number of proposals on how cyber peacekeeping could be designed so that it can assist in maintaining peace and security in the face of cyber warfare. However, many of these proposals lack practical investigation. In this article, we therefore leverage the DSR process to pick out and design just one of these proposals: cyber buffer zones.

Interposition as a buffer zone is one of the core activities of a traditional UN peacekeeping operation. The UN defines a buffer zone as “an area established between belligerents and civilians that is protected and monitored by battalion peacekeeping forces and where disputing or belligerent forces and attacks on each other and the civilian population have been excluded” (United Nations, 2012, p. 92). Peacekeepers keep this buffer zone free from military personnel, weapons, installations and activities and have the authority to use force in order to protect the safety and integrity of the buffer zone (United Nations, 2012).

Robinson et al. (2018, p. 78) adapted this definition to produce a definition of a cyber buffer zone: “A network or site that is protected and monitored by peacekeeping forces, where cyber attacks have been excluded.” They proposed that a cyber buffer zone would be most valuable at sites where the greatest threats to peace exist, and an example of critical national infrastructure was given. These are sites that civilians rely upon for essential services such as electricity, water and transport. A cyber buffer zone could be deployed reactively (i.e. after a suspected attack) or proactively (preventive deployment in anticipation of an attack). The literature regarding buffer zones was distilled down to two core pieces of value which need to be preserved when designing cyber buffer zones:

1. **Deterrence:** Potential attackers are deterred from initiating an attack, due to the high probability of being detected and intercepted (increased chance of failure).
2. **Robust Force Projection:** When deterrence fails, the consequences for an attacker are significant e.g. incarceration, injury or death (increased consequence of failure).

It was suggested that deterrence in a cyber buffer zone can feasibly be achieved in a number of ways. Raising awareness that a particular site is under peacekeeping protection, knowledge that the site will be monitored by highly capable staff, and the increased likelihood of tracing attacks back to their origin could all have the potential to act as a deterrent.

With regards to projecting robust force, an approach which uses both short and long term activities was recommended. Further development of these activities was cited as future work, and this is where this chapter places its focus: proposing how such a cyber buffer zone would technically operate in order to achieve robust force projection and ultimately contribute towards maintaining peace.

SOLUTIONS AND RECOMMENDATIONS

To begin, it is prudent to first become familiar with the activities of a traditional physical buffer zone. The UN has been operating buffer zones for many decades, and this experience provides us with a solid foundation from which to consider cyber buffer zones. The activities they perform in a physical buffer zone have been refined and improved over the years, based upon field experience. We therefore can assume that any activity performed at a UN buffer zone is proven to have value towards restoring peace and is feasible in at least some cases.

The UN Infantry Battalion Manual Volume II (United Nations, 2012) provides a list of the specific tasks that peacekeepers running a buffer zone perform, along with a description of what each task involves. These are presented in Table 1.

Looking at Table 1 we can see that the value a buffer zone brings goes beyond just deterrence and robust force projection. It in fact serves to support multiple other peacekeeping activities ranging from humanitarian assistance to peacemaking. This emphasises the view that the activities of peacekeeping are synergistic: no one activity in itself can restore peace, but together they all work towards a common goal. When designing a cyber buffer zone, opportunities for synergy with the wider peacekeeping operation must be highlighted and encouraged.

An initial practical step in considering the design of cyber buffer zones is to determine if these existing activities could map to a cyber warfare context in a way that would be valuable towards restoring peace. This is our first contribution to knowledge: we take the same table and colour each activity: green if the activity holds potential value in cyber warfare, red if not. The description box is used to show our justification.

Studying Table 2, many of the existing buffer zone activities have potential to bring value as part of a cyber buffer zone. But this is only one piece of the puzzle: it shows there is value to be found but not how to feasibly achieve that value. The second piece of the cyber buffer zone puzzle is how to implement the cyber buffer zone and realise that value in a feasible way.

Looking to the field of cyber security, the concept of securing some infrastructure in the face of cyber attacks is not new. The domain of cyber incident response is a well-established field which can serve as a foundation for implementing a cyber buffer zone. The NIST computer security incident handling guide (Paul Cichonski, 2012) sets out four main tasks of incident response:

- Preparation
- Detection and analysis
- Containment eradication and recovery
- Post incident activity

These guidelines provide a good foundation but do not necessarily apply well to critical infrastructure (Ying, Maglaras, Janicke, & Jones, 2015) or indeed to a cyber buffer zone. For example, in regards to preparation it is suggested that network diagrams and lists of critical assets be created and stored. In the context of a reactive cyber buffer zone, peacekeepers may not have time to collect and study such documents. However, other parts are useful. For example we are reminded that a forensic capability is not only important for later legal proceedings, but also in the immediate concern of providing insight into the current state of the system (Eden, et al., 2016).

Table 1. UN buffer zone activities

TASK	DESCRIPTION
Tactical Deployment	Deploy tactical sub-units and detachments (both permanent and temporary) to effectively cover the entire frontage.
Monitoring	Observe, monitor, supervise and verify the cessation of hostilities/ceasefire/Truce/armistice agreements, compliance of agreements, troop deployments, etc.
Interposition	Interpose between opposing forces to stabilize the situation, where formal peace agreements are not in force.
Supervision	Supervise the implementation of the disengagement agreement.
Repositioning of Belligerent Forces	Accompany and support opposing forces to redeploy/withdraw to agreed dispositions and subsequent adherence to military status quo.
Control of BZ	Ensure no presence of military personnel, weapons, installations and activities, assist in securing the respective areas/line to prevent/intervene entry/intrusion without consent of military personnel, arms or related material in the Buffer Zone.
Civilian Activities	Monitor Crossing/Control Points across buffer zone for safe and orderly passage through by civilians in conjunction with opposing forces. Facilitate daily subsistence and routine activities of civilians in the buffer zone.
Contain	Prevent/contain violations/cross border attacks/isolated incidents taking place and if taken place, prevent it from escalating in to major conflicts.
Investigations	Follow up on complaints by investigations
Proactive Deployment	Proactive troop deployment to prevent an incident or its recurrence
Area of Limitations	Visit, monitor and ascertain compliance of activities periodically in stipulated "Areas of Limitations" (where military restrictions on deployment of body of troops and weapons systems and massing of troops not permitted).
Interface and Coordination	Act as go-betweens for the hostile parties with good liaison, close contact and effective coordination.
Assist Establishment of Local Authority	Assist/coordinate with local Government/belligerent parties in restoring its effective authority in respective areas
Assist in Good Governance	Facilitate good governance in the area of separation/bufferzone, contribute to maintenance and restoration of law and order and policing, establish interface with the inhabitants and help resumption of routine civilian activity (farming, electricity, water, medical support)for establishing normalcy.
Assist other entities	Assist/support formed military police elements, formed UN police elements/UNPOL, UN agencies in the area and other international organizations when tasked.
Mine Awareness	Support mine awareness, identify and mark minefields, and help in clearance of mines and unexploded ordnance.
Facilitate Humanitarian Access	Extend assistance to help ensure humanitarian access to civilian populations, provision of medical aid and facilitate voluntary and safe return of displaced personnel
Reconciliation and Rapprochement	Play an active and constructive role which is critical in preventing a recurrence of hostilities/ to prevent flash point, detrimental to the peace process and work towards a comprehensive political solution.
Assist Negotiation and Mediation	Assist UN mediator and undertake mediation and negotiation when tasked or required.
Other Activities	Facilitate exchange of prisoners, refugees, IDPs, dead bodies and to retrieve livestock.

The US based ICS-CERT(United States Homeland Security, 2009) provides guidance which is more tailored towards industrial control systems and much of the guidance provided can be adapted to help design cyber buffer zones. For example, it describes a number of staffing roles that are necessary including

Table 2. Existing buffer zone activities mapped to cyberspace

TASK	DESCRIPTION FOR CYBER BUFFER ZONE
Tactical Deployment	Deployment of cyber peacekeeping resources to effectively cover the network/site. E.g. experts, monitoring tools.
Monitoring	Use of cyber peacekeeping resources (examples above) to monitor cyber related ceasefire terms.
Interposition	Defend the network from cyber attacks: perform active cyber defence
Supervision	Dependent upon disengagement agreement. But some potential in a cyber context e.g. neutral observation of collaborative efforts to restore control of network to rightful owner or collaboratively remove malware as part of a political agreement.
Repositioning of Belligerent Forces	Cyber troops are difficult to observe and can attack from anywhere. Attempting to monitor or guide their repositioning would not be valuable in a cyber context
Control of BZ	Ensure no presence of cyber attacks and malware. Regular scanning of the infrastructure to ensure it remains clean and free of malicious activity/content.
Civilian Activities	Monitor cyber infrastructure for safe and orderly use by civilians for peaceful purposes. Some infrastructure will be used by civilians for peaceful and essential services. Peacekeepers can ensure the system remains available use e.g. banking, commerce, and government services.
Contain	Prevent or contain cyber attacks from impacting the infrastructure. Isolating and neutralising cyber attacks to avoid escalation into further conflict or relapse into warfare.
Investigations	Follow up on complaints of cyber attack/malware infections (cyber forensic capability)
Proactive Deployment	Proactive deployment of cyber defences to pre-empt and thwart potential attacks
Area of Limitations	Spot checks of networks to ensure that they are not compromised. This could relate to networks that do not have a full time cyber peacekeeping presence but should still be occasionally checked for compromise
Interface and Coordination	Cyber Peacekeepers in a cyber buffer zone can act as go-betweens for the hostile parties
Assist Establishment of Local Authority	Assisting the rightful owner of the network in regaining control e.g. restoring power grid and ensuring no unauthorised access remains
Assist in Good Governance	Advise network owner on how to best protect the network and potentially go beyond security to provide performance/optimisation advice. Long term cyber security capacity building.
Assist other entities	Assist police and other entities e.g. assisting with trace backs, providing cyber forensic capability in case of cybercrime.
Mine Awareness	Identify and contain malware, assist in malware clearance in the network and report on possible malware outside of infrastructure (e.g. detection of external botnet for other teams to follow up on)
Facilitate Humanitarian Access	Potential to protect hospitals from cyber attack, keep routes open (e.g. airport systems, air traffic control) and ensure basic services such as power and water to help humanitarian efforts succeed.
Reconciliation and Rapprochement	Cyber peacekeepers in a cyber buffer zone are unlikely to perform reconciliation duties
Assist Negotiation and Mediation	Some potential to assist wider negotiations through detailed knowledge of the network. E.g. How exposed it is, current events, when can the cyber buffer zone be withdrawn etc.
Other Activities	N/A to cyber peacekeeping

control system engineers, network specialists, system administrators, legal experts and vendor support specialists. This highlights how peacekeepers running a cyber buffer zone must bring expertise from a range of domains to protect the site. However, while we can use this guidance it is also not specific to a peacekeeping environment where one of the primary goals is the protection of civilians (UN Department of Peacekeeping Operations, 2015). Our second contribution is therefore to propose a set of activities for a cyber buffer zone, built using existing guidance where it makes sense but with new proposals where necessary, to suit the goals and conditions of peacekeeping.

We propose that peacekeepers at a cyber buffer zone could conduct three sets of activities following its establishment:

- **Phase One:** Immediate activities
- **Phase Two:** Longer term activities
- **Phase Three:** Withdrawal

PHASE ONE

Phase one consists of the immediate activities. These are rapid and decisive actions designed to gain situational awareness, stabilise the site, address any critical conditions which are an immediate threat to peace and security and restore essential services.

The phase begins by leveraging an existing concept from peacekeeping: a technical assessment mission (TAM) (United Nations Department of Peacekeeping Operations, 2014). In a proactive deployment, this will be a small team of experts who visit the site and assess its suitability for a cyber buffer zone. Since it is a proactive deployment, time will be available to become familiar with the site, collect network maps, asset lists, note observed problems and estimate the expertise that will be required. This is in line with existing guidance relating to the preparation phase of cyber incident response. In a reactive deployment, less time for preparation is available. A rapid response team may be a suitable way to address this problem: a team of peacekeepers who are able to quickly enter a site and perform a rapid assessment. The outcome is to gain situational awareness of the infrastructure, the resources required to secure and stabilise it and a determination on if the site would be suitable for a cyber buffer zone. Some key questions the TAM must answer include:

- Does the peace operation have the required resources to effectively run a cyber buffer zone at this site?
- Would a cyber buffer zone at this site provide value to the wider peace operation (e.g. could failure of the site threaten civilians, lead to state collapse, hamper restoration of state authority...)

If the TAM concludes that the site would be suitable for a cyber buffer zone, a team is established consisting of the required expertise. The process for establishing this team and ways of working (e.g. creation of a war room and communication procedures) can follow best practices described in the ICS-CERT guidance (United States Homeland Security, 2009).

The maintenance of peace and security must remain the overarching priority for a cyber buffer zone. We therefore propose that after establishment, a cyber buffer zone will conduct the following immediate tasks:

Stabilisation –In reactive deployments, a site such as a power plant or water treatment plant may currently be under attack, remotely via a network or locally via malware or insider. An essential task will be to prevent the condition of the site deteriorating. By this we mean working to prevent additional damage which could lengthen the amount of downtime or present a physical threat (e.g. explosion or contamination of water supply). Both of these are critical to avoid, since they are direct threats to peace and security. In proactive deployments where no negative effects are yet observed, the site will already be in a stable condition. Stabilisation will involve the following subtasks:

1. **Situational Awareness:** Both in reactive and proactive deployments, peacekeepers will need to quickly gain situational awareness: an understanding of the infrastructure, its assets, interdependencies, protocols and people. Information collected by the TAM will be useful here as a foundation. Confirmation of what is working and what is failing. Triage of expertise to specific components of the infrastructure for further analysis on the cause of the failures e.g. malware, exploited vulnerability, hardware fault, human error, malicious insider. In the case of attack, the team must determine the attack vector used.
2. **Action Plan:** Once the cyber buffer zone team has gained awareness of the infrastructure, an understanding of where failures are and attack vectors used an action plan can be developed. This plan will aim to directly address the most critical obstacles towards the site being stabilised and assign resources to actions. For example, vendor support experts may be assigned to replace failed hardware whilst malware and forensics specialists work to identify and neutralise malware on engineering stations. Others will be assigned to close the specific vulnerabilities used in attacks. The action plan must be discussed and agreed with all stakeholders, including local staff. Note that tasks one and two will not always be linear: following the action plan the team reassess the site and modify the plan based on new information or a change in the environment.

Phase one can be considered successful when there are no remaining immediate threats to civilians, damage is not spreading, malware has been neutralised (e.g. contained, command and control cut) and actively exploited vulnerabilities have been closed. The team can then proceed to phase two: longer term activities.

PHASE TWO

The goals of this phase are to restore service and establish a long term security capability at the site.

1. **Restoration of Service:** Once a site has been stabilised the next goal is to restore operation and resume provision of the service. Again this will require input from a number of areas including local staff, vendors and experts from the industry in question.
2. **Active Defence:** Once service has been resumed, it will be necessary to monitor the infrastructure and defend against any new attacks. Peacekeepers will deploy cyber defences: IP address blocking, load balancing, reconfiguration and redirecting of denial of service traffic are all examples possible defences. Companies such as Google have expressed interest in assisting the mitigation of denial of service attacks for good causes such as election monitoring groups and human rights organisations (Google, 2016). Organisations such as this would make good partners for a cyber buffer zone and demonstrates how important technology partners could be in making cyber buffer zones effective.
3. **Vulnerability Assessment and Hardening:** With the site stabilised, the team can begin the process of identifying other weaknesses in the security of the infrastructure: known vulnerable or unnecessary software/services, misconfigurations, weak credentials, unnecessary external connections, weak policies, security blindspots, gaps in physical security or human resource security. These are vulnerabilities which threaten the ongoing security of the site, but were not actively being exploited in phase one. Due to the fragile nature of industrial control systems (Wedgbury & Jones, 2015),

vulnerabilities will not be closed until a plan is developed in collaboration with all stakeholders including local staff. The reason for this is twofold: first because patching software or changing long standing configurations may have unexpected consequences upon the operation of the site. Second, local stakeholders need to be engaged and involved in decision making to ensure ongoing cooperation and success of the buffer zone. The end result will be a hardened infrastructure, resilient to future attacks.

4. **Restoration of Control:** The immediate activities focused upon protecting civilians by tackling critical threats, not upon restoring all systems back to the control of the legitimate owner. In this regard, non-critical systems at the site might still be under attacker control even after phase one has completed. This activity aims to restore full control of all systems at the site back to the legitimate owner.
5. **Monitoring and Supervision:** With the immediate threats countered, cyber peacekeepers monitor the site and supervise collaborative efforts e.g. collaboration between two parties to remove malware, arranged as part of a peace agreement.
6. **Cyber Forensics:** Cyber peacekeepers can begin to provide forensics services to identify how breaches occurred and what information was stolen etc. This is useful for verifying ceasefire agreements and for third party enquiries such as national police.
7. **Peace Support:** Cyber peacekeepers can use their knowledge of the site and its staff to support wider peacekeeping tasks. For example they can provide evidence on compliance with cyber terms, report upon ongoing attacks from external sources, act as an intermediary between the hostile parties, support police investigations and share information on malware which may be valuable for other cyber buffer zones in a region.
8. **Training:** Local staff are trained in security best practices specific to the infrastructure they are maintaining, for example developing incident response plans relevant to industrial control systems. The goal is to build a local capability so that peacekeeping forces can proceed to phase three and withdraw from the site.

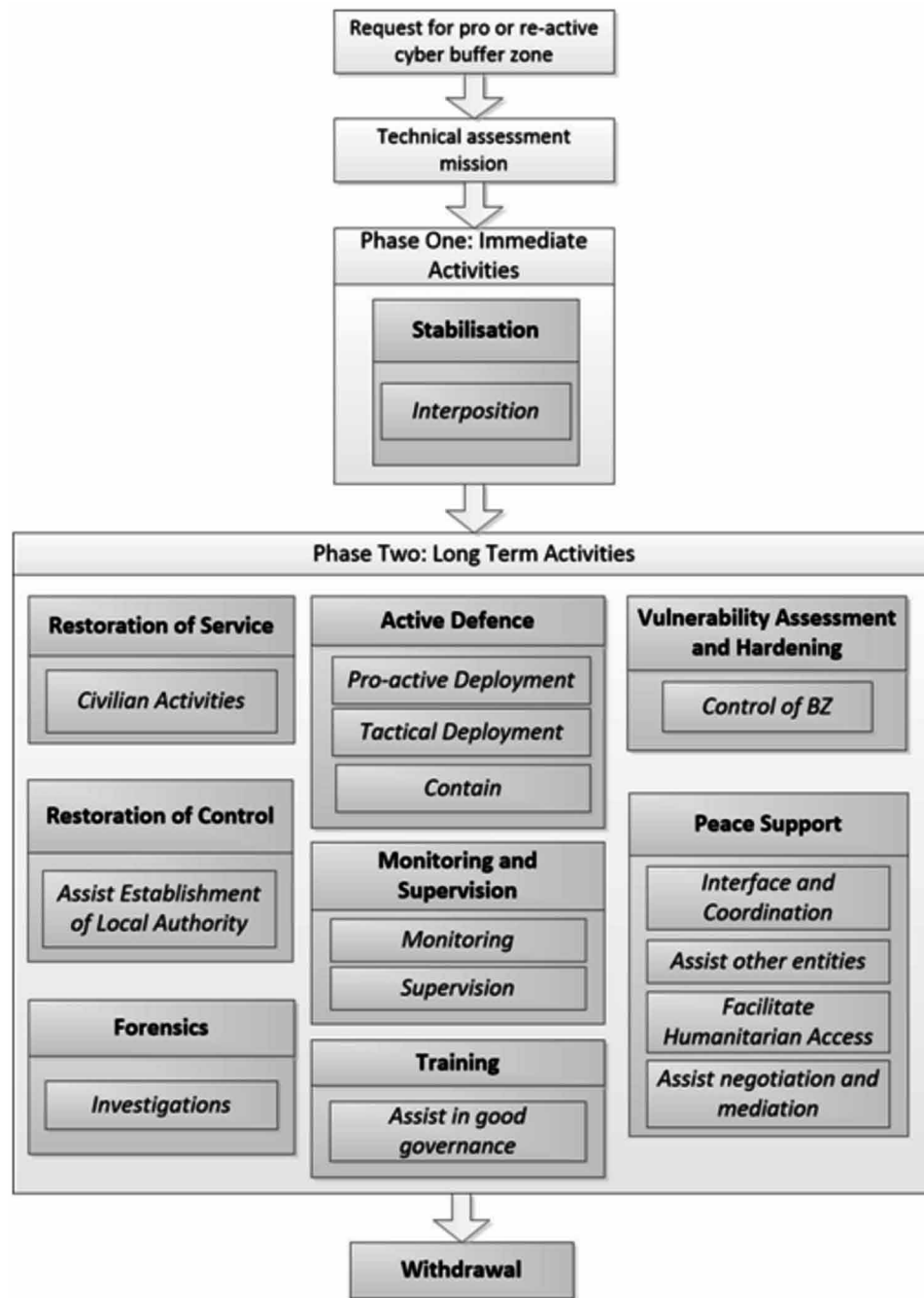
Phase two activities will continue until local staff are able to maintain the security of the infrastructure without cyber peacekeeper assistance. This goal is in line with existing peacekeeping doctrine, which strongly encourages local capacity building to enable eventual withdrawal of UN forces (United Nations, 2008).

PHASE THREE

Withdrawal: The eventual goal of peacekeepers, in all domains, is to build a local security capability and hand over responsibility for security to local staff. A cyber buffer zone will be no different: peacekeepers cannot stay at the site forever, and must eventually withdraw once a local capability has been built. This local capability should be effective enough to ensure the site is well protected in the long term. Activities in phase two are designed to contribute towards this: hardening of the site and training are both activities which aim to enable eventual withdrawal of cyber peacekeeping services.

A visual representation of the three phases, along with how each activity maps to the existing activities of a physical buffer zone is presented in Figure 1.

Figure 1. The three phases of a cyber buffer zone (own synthesis)



CONCEPT EVALUATION - FUTURE RESEARCH DIRECTIONS

The proposals made in this article are crafted to fulfil the goals of a UN peace operation (namely, to protect civilians) whilst remaining feasible to perform. In this section, we discuss where obstacles may arise and avenues for future research.

Local Resistance

The success of a cyber buffer zone as described in this article is highly reliant upon the cooperation of local staff. Cyber peacekeepers will find it difficult to perform the activities we describe if local staff do not provide assistance, or actively resist. Cooperation of local staff should be measured by the technical assessment mission, and a lack of cooperation is grounds for denying a buffer zone. Unfortunately this could place the UN in a difficult situation. For example, in a case where critical infrastructure is failing to the point where it presents a threat to civilians yet local cooperation is lacking. This is a challenging scenario where future research would be welcomed.

Lack of Consent

While local resistance represents an unwillingness to cooperate at the field level, we must also consider a lack of consent at higher levels. Consent of the parties is one of the core principles of UN peacekeeping (United Nations, 2008), and is required for the success of the operation. Take a scenario where critical infrastructure is failing and threatening civilian security, and local staff appear to be unsuccessful in tackling the threat. The UN may feel that a cyber buffer zone is critical for peace and security in the region but may find that consent is not given by the host nation. Following existing doctrine, this naturally leads to the question of peace enforcement.

Peace enforcement has been used in the past for the following purposes (Bellamy & Williams, 2010):

- To restore or maintain international peace and security.
- To enforce sanctions.
- To defend peacekeeping personnel.
- To provide physical protection to civilians.
- To protect humanitarian activities.
- To intervene in internal conflicts.

It is therefore not radical to propose that the UN has the option to forcefully impose a cyber buffer zone at CNI which threatens the physical security of civilians or the maintenance of international peace and security. The importance of the UN's authority to enforce peace was supported by ex-secretary general Boutros-Ghali who stated that "while such action should only be taken when all peaceful means have failed, the option of taking it is essential to the credibility of the United Nations as a guarantor of international security" (United Nations, 1992, p. 12). If it is agreed that the authority to enforce a cyber buffer zone exists, it must be asked if it would be feasible. This would be a valuable area for future work.

Ensuring Impartiality

Impartiality is the second core principle of UN peacekeeping, and must be upheld when establishing cyber buffer zones. Ensuring that a buffer zone is impartial, and is seen as such, may become a challenging task. This is because cyber peacekeepers are taking an active role: bolstering defences, training staff and restoring control. Care must be taken to ensure that any buffer zone has the clear, publicised aim of protecting civilians. It is necessary to emphasise that they will only be established at sites where a lack of protection could endanger the human rights of civilians. Military sites and systems will not be protected. It must also be made clear that a buffer zone is focused upon defence, and not offence.

A potential threat to the appearance of impartiality is that establishing a UN cyber buffer zone to protect CNI frees up that nation's cyber troops to focus upon offence rather than defence. This has the potential to lead to undesirable incentives such as letting CNI fail or purposely creating incidents so that the UN will step in and provide protection. This is a valid concern that must be considered. One response is to only provide a buffer zone once peace has been agreed. If a nation then wishes to cheat and continue offensive cyber operations while enjoying the benefits of the buffer zone, this is a risk that could result in consequences on the international stage.

The problem of resource hoarding also exists. Country A may request many cyber buffer zones simply to consume UN cyber resources and deny the service to its rival. Cyber peacekeeping resources must therefore be provisioned in a balanced manner, with restraint in mind. The technical assessment missions will be crucial here, to decline requests where there is no clear need. The protection of civilians will always be the greatest deciding factor regarding where cyber buffer zones are established.

Securing Critical National Infrastructure

It has been argued that cyber buffer zones will likely bring most value when established at a critical national infrastructure (CNI). It is a known issue that the hardware, software and protocols which operate CNI are particularly challenging to secure from a cyber perspective. Firstly they make attractive targets to a wide spectrum of attackers. Nation states, terrorist groups, hackers, activists, organised crime and disgruntled insiders all potentially have an interest in attacking CNI (Robinson, 2013). Secondly, the technology used at such sites is known to possess characteristics which make it particularly vulnerable to cyber attack and challenging to defend (Merabti, Kennedy, & Hurst, 2011). A discussion into all of the security issues of CNI is beyond the scope of this paper, but extensive literature exists in this area (Robinson, 2013) (Gao, et al., 2014) (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). Instead, we will highlight challenges that present a specific problem to a cyber buffer zone.

Arguably one of the major challenges peacekeepers will face in building a cyber buffer zone will be to work with the hardware, software and protocols. These components can be decades old, built using proprietary technologies, fragile in their operation and designed/tested in an isolated environment. These characteristics will make establishing a cyber buffer zone at CNI much more challenging than in a traditional ICT environment.

To give a concrete example, let us consider phase one. During this phase, the peacekeepers aim to stabilise the infrastructure by identifying where critical negative effects are originating from and resolving the issue. At a traditional ICT based environment, this would involve the use of various monitoring tools. The NIST guidance suggests the use of network and host-based IDPSs, antivirus software and log analysers (Paul Cichonski, 2012). Research suggests that using such tools at CNI could have negative effects on the functioning of core components, causing them to become unresponsive, slow or unpredictable in behaviour (Coffey, Smith, Maglaras, & Janicke, 2018). It is also rare for such components to hold any logs or other forensic artefacts of value which can be retrieved (Eden, et al., 2016). Even the act of closing a vulnerability through patching firmware, software or making a configuration change could be enough to cause unexpected results which worsens the situation. The conclusion we must reach is that peacekeepers entering CNI to establish a buffer zone will require very specific skillsets in order to correctly diagnose and remediate cyber incidents without making the incident worse.

Gaining Situational Awareness

In the case of a reactive cyber buffer zone, peacekeepers may be asked to deploy with no or limited pre-existing knowledge of the site's hardware, software and protocols. This makes gaining situational awareness of the infrastructure an important task but difficult task. The age of the components at the site make it possible that the vendor who produced them is no longer in business. This immediately presents an obstacle towards finding expertise, documentation and replacement parts. Network diagrams may be missing or inaccurate. In the context of a warfare environment, local staff who could share knowledge may be absent. A site suffering negative effects which are directly harming civilians (e.g. faulty water treatment) will also place pressure upon the team to act quickly. Work which explores how a cyber buffer zone team can quickly gain knowledge and situational awareness of critical infrastructure under these conditions would therefore be valuable.

Difficulty to Train

Peacekeepers working on other activities can perform training to prepare themselves for deployment in the field. For example, exercises can be run to simulate a physical buffer zone and the types of scenarios they could face. Simulating a cyber buffer zone for training purposes will be more challenging. Due to the problem of fragility at CNI and a 100% uptime requirement, the UN will have difficulty finding a site where cyber peacekeepers can test their tools and processes. Simulations are a possible solution here, but producing such a simulation, which could accurately model cyber warfare's effects on critical national infrastructure and its components is a complex task. Efforts in this area do exist (Ferreira, Machado, Costa, & Rezende, 2015) but further research would bring value to developing effective cyber buffer zones.

Securing Cyber Expertise

Cyber security expertise is in high demand across the world, with some estimating that by 2021 there will be 3.5 million unfilled cyber security roles across the public and private sector (Morgan, 2017). With threats in cyber space only rising, the demands for staff with cyber expertise will only continue to grow. This presents a challenge to the concept of cyber peacekeeping: where is the expertise going to come from and how will it be funded? Peacekeeping organisations such as the UN rely upon contributions of troops from member states, but it is questionable if states already short on cyber expertise would be willing to lose them to support a peace operation. We have also proposed that a cyber buffer will need a range of skillsets, including some which come from the private sector. It must therefore be asked what incentives these private organisations would need to contribute their expertise. Research on why states contribute towards peace operations is well established (Bove & Elia, 2011) (Bellamy & Williams, 2013), and it would be useful to explore how this body of work can be applied to the concept of cyber buffer zones.

Political, Legal and Social Concerns

The concept of peacekeeping is one which touches upon multiple domains of thought. Legal, social, political and military considerations all come together to make peacekeeping a success. A cyber buffer zone will be no different. Studies which examine the legal implications and requirements will be es-

sential. For example, it is likely that many sites critical to the protection of civilians will be owned by private entities and not the nation state itself. This raises questions about a state's ability to consent to a buffer at sites it does not outright own. Questions of privacy, data protection and ethics may also arise in the case of peacekeepers of multiple nationalities entering infrastructure to perform monitoring of network traffic. On the political aspect, highly cyber developed nations may be wary of sending their cyber experts to work alongside those from rival nations. There is even the possibility for cases where a nation is conducting or condoning cyber attacks on one hand, whilst contributing cyber peacekeepers with the other. In this regard there is potential for the goals of a cyber buffer zone to become subverted for ulterior motives, or at least for the suspicion of such to exist between nations. Research which explores and resolves these aspects is valuable towards making cyber buffer zones a success.

CONCLUSION

UN Peacekeeping has been operating since 1948, working to maintain peace and protect civilians around the world, and buffer zones in particular have featured throughout the history of UN peacekeeping as a means to physically separate conflicting forces, protect civilians and ensure peace in a region. As war increasingly gains a cyber component, it is important to consider how peacekeeping must adapt to remain effective. The field of cyber peacekeeping addresses this issue, and in this chapter we have made a contribution by proposing a possible design of a cyber buffer zone, based upon a three phase approach. This approach was built by fusing together knowledge from both the cyber security and peacekeeping domains.

We critically evaluated our design against two core criteria: that it should be feasible to perform and provide some kind of tangible benefit to peace. From the perspective of value, a cyber buffer zone can directly address one of the main goals of UN Peacekeeping: protection of civilians. As societies become increasingly reliant upon cyber space for the provision of services such as power, water, finance, transport and commerce, the impact that cyber warfare could have upon these services rises. Failure of a smart grid, air traffic control or the rail network could at the very least prevent a nation and its citizens from recovering to a level where peace can be maintained. In some cases, it could lead to loss of life.

We have therefore designed cyber buffer zones as an activity which consists of both immediate and longer term activities. The focus of the immediate activities is to rapidly address any pressing threats to civilians and peace. Once this has been achieved, cyber security at the site is bolstered so that it remains resilient into the future.

While a cyber buffer zone is valuable, we have shown that there are many challenges to overcome in relation to feasibility. Critical national infrastructure can be difficult to secure, especially at short notice without much prior knowledge of the hardware, software and protocols in use. It will also require specific expertise that will likely be expensive in a market where cyber expertise is in high demand. Our solution proposal to the problem of developing cyber buffer zones is therefore not perfect: it requires further work and input from the research community, and for alternative designs which can overcome or reduce these obstacles. In this regard, it is hoped that this work can serve as a discussion point from which further progress can be made.

REFERENCES

- Akatyev, N., & James, J. I. (2015). *Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. Revised Selected Papers*. Springer International Publishing.
- Baradaran, N., & Habibi, H. (2017). Cyber Warfare and Self-Defense from the Perspective of International Law. *J. Pol. & L.*, 10, 40.
- Baskerville, R. (2008). What design science is not. *European Journal of Information Systems*, 17(5), 441–443. doi:10.1057/ejis.2008.45
- Bellamy, A., & Williams, P. (2010). Understanding Peacekeeping. *Polity*.
- Bellamy, A., & Williams, P. (2013). *Providing Peacekeepers: The Politics, Challenges, and Future of United Nations Peacekeeping Contributions*. OUP. doi:10.1093/acprof:oso/9780199672820.001.0001
- Bove, V., & Elia, L. (2011). Supplying peace: Participation in and troop contribution to peacekeeping missions. *Journal of Peace Research*, 48(6), 699–714. doi:10.1177/0022343311418265
- Cahill, T. P., Rozinov, K., & Mule, C. (2003, 6). Cyber warfare peacekeeping. In *Information Assurance Workshop*, 2003. *IEEE Systems, Man and Cybernetics Society*, (pp. 100-106). IEEE.
- Coffey, K., Smith, R., Maglaras, L., & Janicke, H. (2018). Vulnerability Analysis of Network Scanning on SCADA Systems. *Security and Communication Networks*, 2018, 1–21. doi:10.1155/2018/3794603
- Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics*, 9(4), 384–410. doi:10.1080/15027570.2010.536404
- Dorn, W. (2017). *Cyberpeacekeeping: A New Role for the United Nations?* (Vol. 18). Georgetown Journal of International Affairs.
- Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., & Soulsby, H. (2016). A Cyber Forensic Taxonomy for SCADA Systems in Critical Infrastructure. In E. Rome, M. Theocharidou, & S. Wolthusen (Eds.), *Lecture Notes in Computer Science: Vol. 9578. Critical Information Infrastructures Security. CRITIS 2015* (pp. 27–39). Springer. doi:10.1007/978-3-319-33331-1_3
- Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H., . . . (2016). Forensic readiness for SCADA/ICS incident response. In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research* (pp. 1-9). Swindon, UK: BCS Learning & Development Ltd. 10.14236/ewic/ICS2016.16
- Ferreira, A., Machado, A., Costa, F. A., & Rezende, J. L. (2015). Use of simulation to achieve better results in cyber military training. *IEEE Military Communications Conference*.
- Gao, J. J., Rajan, B., Nori, R., Fu, B., Xiao, Y., & Liang, W. (2014). SCADA communication and security issues. *Security and Communication Networks*, 7(1), 175–194. doi:10.1002/ec.698
- Google. (2016). *Project Shield*. Retrieved from <https://www.google.com/ideas/products/project-shield/>
- Kleffner, J. K., & Dinniss, H. A. (2013). Keeping The Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, 89, 512–539.

- Liles, S., Rogers, M., Dietz, J. E., & Larson, D. (2012). Applying traditional military principles to cyber warfare. In *Cyber Conflict (CYCON), 2012 4th International Conference on*, (pp. 1-12). Academic Press.
- Martins, R. P. (2018). 4). Punching Above Their Digital Weight. *International Journal of Cyber Warfare & Terrorism*, 8(2), 32–46. doi:10.4018/IJCWT.2018040103
- Merabti, M., Kennedy, M., & Hurst, W. (2011). Critical infrastructure protection: A 21st century challenge. *International Conference on Communications and Information Technology*.
- Morgan, S. (2017). *Cybersecurity Jobs Report 2018-2021*. Cybersecurity Ventures.
- Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, 31(4), 418–436. doi:10.1016/j.cose.2012.02.009
- Paul Cichonski, T. M. (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology.
- Robinson, M. (2013). The SCADA Threat Landscape. In *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013* (pp. 30-41). BCS.
- Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, 49, 70–94. doi:10.1016/j.cose.2014.11.007
- Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, 114, 70–87. doi:10.1016/j.jnca.2018.04.010
- Rrushi, J. L. (2012). SCADA Protocol Vulnerabilities. In J. Lopez, R. Setola, & S. D. Wolthusen (Eds.), *Critical Infrastructure Protection* (pp. 150–176). Berlin: Springer-Verlag. doi:10.1007/978-3-642-28920-0_8
- Ruiz, M. (2017). Establishing volunteer US cyber defense units: A holistic approach. In *International Conference on Cyber Conflict (CyCon U.S.)* (pp. 45-58). Washington, DC: IEEE. 10.1109/CYCONUS.2017.8167512
- THIBER (The Cybersecurity Think Tank). (2013). *Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales*. Universidad Autónoma de Madrid.
- UN Department of Peacekeeping Operations. (2015). *The Protection of Civilians in United Nations Peacekeeping*. United Nations.
- United Nations. (1992). *An Agenda for Peace A/47/277*. Author.
- United Nations. (2008). *United Nations Peacekeeping Operations: Capstone Doctrine*. Author.
- United Nations. (2012a). *United Nations Infantry Battalion Manual* (Vol. 1). United Nations.
- United Nations. (2012b). *United Nations Infantry Battalion Manual* (Vol. 2). United Nations.
- United Nations Department of Peacekeeping Operations. (2014). *Planning Toolkit*. United Nations.
- United States Homeland Security. (2009). *Developing an Industrial Control Systems Cybersecurity Incident Response Capability*. Author.
- Vaishnavi, V., & Kuechler, B. (2015). *Design Science Research in Information Systems*. Academic Press.

Wedgbury, A., & Jones, K. (2015). Automated Asset Discovery in Industrial Control Systems - Exploring the Problem. *3rd International Symposium for ICS & SCADA Cyber Security Research*. 10.14236/ewic/ICS2015.8

Ying, H., Maglaras, L., Janicke, H., & Jones, K. (2015). An Industrial Control Systems incident response decision framework. *IEEE Conference on Communications and Network Security*. 10.1109/CNS.2015.7346923

ADDITIONAL READING

Akatyev, N., & James, J. I. (2015). Cyber Peacekeeping, Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. Revised Selected Papers. In I. J. James, & F. Breitingner (Eds.). Springer International Publishing.

Bellamy, A., & Williams, P. (2010). Understanding Peacekeeping. *Polity*.

Dorn, W. (2017). *Cyberpeacekeeping: A New Role for the United Nations?* (Vol. 18). Georgetown Journal of International Affairs.

Kleffner, J. K., & Dinniss, H. A. (2013). Keeping The Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, 89, 512–539.

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2018). *Threats, Protection and Attribution of Cyber Attacks on National Critical Infrastructures*. EAI Transactions on Security and Safety.

KEY TERMS AND DEFINITIONS

CNI: Critical national infrastructure.

DDR: Disarmament, demobilisation, and reintegration.

UN: United Nations.

The Management of Whistleblowing

Riann Singh

The University of the West Indies, St. Augustine, Trinidad and Tobago

Shalini Ramdeo

The University of the West Indies, St. Augustine, Trinidad and Tobago

INTRODUCTION

Within the last two decades, corporate scandals, fraud and corruption, unethical and illegal business practices, misconduct in the workplace, malpractice, and the mismanagement of funds have all been associated with corporate wrongdoing in the public and private sectors. Indeed, such a business context has arguably led to disgruntled employees, poor company images, and many publicized corporate melt-downs within powerhouse corporations across the globe. The effect of corporate failures brought devastating effects to the global economy as triggers to the economic recession in 2008. Undeniably, therefore, corporate wrongdoing must be brought under control within today's workplace for all organizations.

Effective control of corporate wrongdoing within today's workplace calls for clear, structured, accepted, and well-managed procedures to facilitate whistleblowing. A managerial perspective must therefore, be adopted to systematically establish and support whistleblowing. In the corporate context, whistleblowing can be defined as a disclosure process which uses various channels (internal and/or external) for organizational members (past or present) to report illegal, immoral or illegitimate practices within an organization, with the aim of stopping or addressing the harm or threat (Near and Miceli 1985). Immoral practices also cover wrongful and questionable commissions and omissions on the part of the organization to protect their members from serious harm (Near and Miceli 1996). In this regard, whistleblowing can assist in rooting out corruption and wrongdoing by bringing such issues to the forefront. Whistle-blowers should therefore, be seen as heroes since they can assist in saving billions of dollars and numerous lives through the disclosure of information regarding fraud, corruption, and other forms of corporate wrongdoing and misconduct by organizations, thereby protecting citizens, employees and consumers, and preventing related disasters and scandals from intensifying.

Despite the potential of whistleblowing as a process for managing corporate wrongdoing, its effectiveness has often been brought into question by opponents due to several reasons. First, the decision to report the observed wrongdoing is never an easy one, given the high personal costs, which can deter whistleblowing. In some contexts, whistle-blowers can be regarded as heroes, while in others, they can be perceived as traitors and snitches. Second, organizational leaders and management can respond in a number of different ways, which may or may not be favourable to the reporter or whistle-blower. Managerial responses can include: correcting the wrongdoing, ignoring the report, or even retaliating against the whistle-blower. Positive managerial responses can signal to employees that management accepts the whistleblowing behaviour in the organization and is prepared to curb the wrongdoing. Negative managerial responses in the form of victimization and/or no action can serve as a disincentive to

whistleblowing. In such a context, it is apparent that the effectiveness of whistleblowing in addressing corporate wrongdoing can be limited. To maximize the potential of whistleblowing, therefore, it becomes important to answer the question: “How can organizations manage whistleblowing to effectively address corporate wrongdoing in today’s business environment”? To answer this question, the research objectives of this Chapter are to:

- Describe the key management issues associated with whistleblowing.
- Outline the essential aspects of the ethical dilemma in the management of whistleblowing.
- Present and evaluate a managerial framework to enhance the effectiveness of whistleblowing.

BACKGROUND

Recent failures of corporate integrity among high-profile organizations have emphasized the need to prevent, detect, and respond to corporate wrongdoing that can lead to devastating consequences for economies, businesses, employees, and other stakeholders. Whistleblowing in today’s corporate world is increasingly becoming a mainstream issue, since it is the key component in promoting a culture of integrity. Whistleblowing generally describes the process through which corporate wrongdoing can be exposed; where exposure should set the stage for managing and minimizing such wrongdoings. The range of activities that may constitute corporate wrongdoing include, but are not limited to: corruption, bribery, receiving and giving gifts and entertainment, kickbacks, extortion, nepotism, favouritism, cronyism, money laundering, improper use of insider information, insider trading, conflicts of interest, fraud, discrimination, aggressive accounting, sexual harassment, workplace safety, product safety, and environmental pollution (Near and Miceli 1996). All definitions of whistleblowing establish that it involves the reporting of such wrongdoing, that wrongdoing is not confined to illegality, whistleblowing is not confined to reporting to fellow employees, and whistleblowing should encourage persons to report activities that may be fraudulent or harmful to the business and stakeholders (Near and Miceli 1996).

Notably, whistleblowing can be done via internal and external channels. If an alleged wrongdoing is reported to internal authorities, such as, persons in positions of authority within an organization, audit committees, or anonymous channels, it is referred to as internal whistleblowing. If an alleged wrongdoing is reported to outside authorities, such as, regulatory bodies, news media, or public interest groups, it is referred to as external whistleblowing. There is some consensus that whistle-blowers may prefer to blow the whistle through available internal channels. However, most employees may be too scared to blow the whistle internally for fear of victimization, retaliation, reprisal or even dismissal. Fletcher, Sorrell, and Silva (1998) in their research on whistleblowing note an important case study which highlights clearly some of the issues that could emerge using even internal whistleblowing channels.

In 1996, in a New England hospital, a registered nurse Barry Adams blew the whistle using internal channels on unsafe health care practices he observed in his workplace. He documented the unsafe practices and noted instances where patient safety, healthcare and well-being were being compromised. For three months, such practices were documented and reported to internal hospital administrators using the prescribed processes and procedures. However, Adams soon realized there was little to no interest in correcting the unsafe practices, no interest in using the information to do so, and in fact, he was harshly

criticized for collecting such information. Adams subsequently took a different approach by refusing to participate in acts that were contrary to established legal and ethical practices, for example, he refused to take narcotics orders from a physician's technician, citing its contradiction with legislation such as the Nurse Practice Act. The response; Adams was threatened, and although he had a track record of excellent performance reviews, he was eventually fired. Adams took this matter to court and won his case; subsequent appeals by the hospital were turned down.

From the case, it is evident that even internal whistleblowing can have undesirable consequences for the whistle-blower, which may nullify benefits that could be derived from the disclosure of corporate wrongdoings. Many employees in today's corporate world, as well as, other organizational stakeholders may be hesitant to report any perceived corporate wrongdoing, since they can become stuck in what is referred to as the "whistle-blower's dilemma". Here, the reporter is faced with the predicament of weighing the positive impact of his impending revelation and the possible dangers to his life, family, reputation, and profession. Such reporters generally may not feel adequately protected to come forward with information on misconduct and corrupt practices. Where reports are made, as seen in the New England case, they can face retaliation, victimization, intimidation, recrimination by supervisors or co-workers, denial of work-related benefits, suspension from work, and at times, outright dismissal. These negative consequences can lead to low participation in the internal whistleblowing process as an avenue for the disclosure and management of corporate wrongdoing.

Fletcher, Sorrell and Silva (1998) further make a number of important points with the New England case study that while there may be problems with internal whistleblowing; such problems emerge largely due to the failure of organizations to follow and act on documented ethical guidelines/policies to safeguard the interest of all organizational stakeholders, and that external whistleblowing could only possibly be considered an option when there is a failure of internal organizational ethics. In fact, whistleblowing itself should not even occur if there are effective internal procedures to address staff concerns within an ethical organization. If the organizational ethics and internal procedures were effective at the New England hospital, the unsafe practices would not have been tolerated and Adams would not have unsuccessfully exhausted the internal channels of communication before taking legal recourse for his wrongful dismissal, following his whistleblowing.

When all is said and done, it is important that the whistle-blower blows the whistle for the morally right reason; preserving the safety and welfare of all concerned, and not for selfish personal gains. Registered Nurse, Barry Adams appeared to have the safety of the patients at heart in his disclosure in the 1996 whistleblowing case. From a deontological view, Adams's duty to the safety of patients supersedes his duty or loyalty to such an organization. Studies consistently show that whistle-blowers are motivated by moral reasons. The primacy of moral concerns makes sense, considering how frequently whistle-blowers face exclusion and retaliation rather than personal gain. For example, more recently, in May 2015, the Securities and Exchange Commission (SEC) punished Deutsche Bank with a \$55 million fine. Deutsche's crime was inflating the value of its portfolio of complex derivatives by \$1.5 billion during the financial crisis. The SEC promised former Deutsche Bank risk analyst, Eric Ben-Artzi, \$8.25 million for his role in exposing this overvaluation by providing documents to regulators. This payout resulted from the whistle-blower program introduced under the 2010 Dodd-Frank law, which rewarded eligible individuals who voluntarily provide information leading to successful sanctioning of over \$1 million. Depending on the case, whistleblowers could receive 10 to 30 percent of the sanctions collected. The

rationale behind this program was to motivate organizational members to come forward to expose corporate wrongdoing. Indeed, Ben-Artzi noted when he first began helping the SEC with their investigation the prospect of a financial reward was a “powerful incentive.” Except, stunningly, Ben-Artzi refused to accept his payout, explaining that he was willing to forego his multi-million dollar reward because the top executives responsible for Deutsche’s crime went completely unpunished and instead retired with multi-million dollar bonuses. Under the Dodd-Frank whistleblowing program, vindication is generally rare as well. As of last year, the SEC had awarded only 22 whistle-blowers despite receiving 14,116 tips since the whistle-blower program’s inception (Duncan, Waytz and Young 2015). Ben-Artzi’s case illustrates that the motivations of whistleblowers extend far beyond practical concerns and financial gains, and also sheds light on the limited functionality of the current U.S. whistle-blower program. It is therefore, apparent that ethical and legal conflicts can impact the effectiveness of whistleblowing to address corporate wrongdoing as well. The Deutsche case and the failure of prosecutors to punish the wrongdoers following the disclosure of Ben-Artzi demonstrate the need for stronger legislative frameworks to fully support the whistleblowing process and to address legal loopholes.

Whistleblowing indeed presents an ethical dilemma for observers of corporate wrongdoing and De George (1986) presents the key aspects of this ethical dilemma in three perspectives: whistleblowing as morally prohibited, morally permitted and morally required. The most common argument for not blowing the whistle is loyalty. However, loyalty or duty to one’s organization of employment or organization of interest as an argument against whistleblowing ignores the norms of a democratic society, the freedom of speech and the ethical notion that absolute loyalty to any entity or anyone does not exist in reality. Loyalty to one’s organization within one’s employment agreement does not ethically allow the observer to ignore practices and policies that could cause serious harm to others within or outside private and public organizations. Whistleblowing is in fact morally permitted under a number of conditions which permeate today’s workplace. For instance, if customers, innocent bystanders, or the general public may be seriously harmed in any way by an organization’s products, services, practices or policies, the disclosure of such wrongdoing should be permitted. In such a case, if one’s immediate supervisor is passive about the disclosure or complaint, the employee should then exhaust the internal procedures and possibilities within the organizational hierarchy to make his concern known (De George 1986). Whistleblowing then becomes absolutely required when the whistle-blower has access to documented evidence to convince an independent, reasonable, impartial observer that the company’s products, services, practices or policies poses a serious threat to customers, bystanders or the general public. Therefore, the probability that the wrongdoing would be managed, upon disclosure, must be worth the risk and danger being taken by the whistle-blower in exposing the threat or harm. Drawing from the case of wrongdoing at the New England hospital, it is clear that Barry Adams did no wrong as a whistle-blower, following documented internal procedures for disclosure, and whistleblowing was indeed absolutely required with documented evidence of unsafe health practices at the hospital. Even so, whistleblowing in this instance was unsuccessful in addressing the unethical and illegal practices identified. It is therefore, apparent that there is a need for a comprehensive management framework to maximize the power of whistleblowing to address corporate wrongdoing, while addressing the challenges that can negatively impact its effectiveness.

FOCUS OF THE ARTICLE

Management Framework for Whistleblowing

When developing a comprehensive managerial framework for whistleblowing, and to maximize its benefits to address corporate wrongdoing, the key aspects of the whistleblowing process must be clearly outlined, well-detailed, openly communicated, and widely accepted.

The Whistleblowing Process

From a managerial perspective, there are four key aspects to whistleblowing:

1. The identification that the act is wrongful and can cause harm
2. THE decision to report the wrongdoing
3. the organizational response to managing, addressing and ending the wrongful acts
4. The organizational response to the whistle-blower

Identification of Corporate Wrongdoing

Firstly, what constitutes corporate wrongdoing must be clearly articulated by private and public organizations. Organizations can no longer rely exclusively on internal codes of conduct and ethical structures to prevent all unethical behaviour, but have to depend to some degree on individuals who are willing to blow the whistle if they detect illegal, dangerous or unethical activities as well. Generally, corporate wrongdoing falls into the following categories: criminal offences, the failure to comply with obligations outlined by organizational policies and law, any miscarriage of justice, endangering of employees, stakeholder or public health and safety, damage to the environment, and the covering up or ignorance of wrongdoing in any of the aforementioned areas (Near and Miceli 1996). More recently, managers and researchers have articulated the need for more clarity in what specific acts constitute corporate wrongdoing, and hence, what acts can be exposed through whistleblowing channels and mechanisms. For example, corruption and fraud are more clearly identifiable as illegal acts. Unethical acts such as conflicts of interest however, may not be clearly identifiable as corporate wrongdoing, although such acts can also cause serious harm to organizational stakeholders and the general public. It is therefore, crucial that public and private organizations establish and publish a domain of acts, which pose a threat or harm to human safety and well-being.

Reporting of Corporate Wrongdoing

Putting measures in place to detect wrongdoing in organizations is important, but reporting to correct wrongdoing is also vital (Kaptein 2011). Employees who detect wrongdoing should, therefore, be encouraged to respond in a manner that supports corrective action. Whistleblowing is contrary to the tradition that an employee does not question a superior's decisions and acts, especially not in public. What is at stake is the employee's right to speak out in cases where they think the organization or management is

engaging in an unacceptable practice that could harm other employees, the welfare of the organization, innocent bystanders, the environment, and/or the public. If employees conclude that they cannot discuss or report current or potential unethical activities with co-workers or superiors, they may go outside the organization for assistance to address such wrongdoings. This is where decisions must be taken to report or not to report, to report internally or externally, or to leave the organization; decisions which are never easy for the observer.

The decision to stay silent and/or leave the organization both close the door to the benefits of whistleblowing as a mechanism for exposing and rooting out corporate wrongdoing. Further, reporting internally or externally both opens the door to maximize the benefits of whistleblowing, while also raising issues of protection for the observers. There has been some consensus among researchers that internal whistleblowing is preferred by most whistle-blowers and most organizations; a point acknowledged before. Internal whistleblowing gives the organization an opportunity to solve the problem behind closed doors and in internal way. In some cases, internal whistleblowing may even be perceived as the employee exhibiting loyalty and commitment to their organization. The success of internal whistleblowing, however, depends on its acceptance by the organization and its members, as well as, the organization's openness to and acceptance of disclosure.

According to Berry (2004), the ethical culture of organizations also plays a crucial role in stimulating employees to report wrongdoing internally, with the expectation that the practices can be corrected and the infractions can be addressed. Ray (2006) went on in her study to detail a case where all internal whistleblowing through the hierarchy of the organization failed, similar to the New England case of Barry Adams; however, external whistleblowing was used, because ethical standards were clearly contravened and organizational ethics failed. She argued that an organization that does not support those that whistleblow because of a violation of professional standards is indicative of a failure of organizational ethics. In that case, it was observed that a nurse told patients of schizophrenia within an acute care psychiatric facility that she could 'cure' their mental illness by the laying on of hands, which she proceeded to do both individually and in groups. She was not practicing therapeutic touch but physically touching the patients on various parts of their bodies without their consent. After these sessions the patients were visibly upset and required medication to help them to settle down. After reporting through the organizational hierarchy failed, the matter was reported externally to the Canadian Nurses Association and the College of Nurses of Ontario (CNO) for action, since the reported practices clearly contravened Codes of Ethics and Standards of Practice. When employees report organizational misconduct through external channels, it can create havoc within the company in the public domain. However, external whistleblowing becomes an option for whistle-blowers when the ethical culture of the organization largely fails to take corrective action through internal whistleblowing. It is therefore important for management frameworks to focus on building a strong ethical climate or a moral community within organizations as Ray (2006) states. Within a moral community, there is no gap between what employees know is the right thing to do and what they actually do. Developing a moral community means using strong values and ethical beliefs to guide organizational decision making and practices. A relational view may therefore be more effective within the management of whistleblowing by fostering an interdependent moral community to address ethical concerns.

Where infractions do occur however, anonymous whistleblowing may be preferred to whistleblowing where the reporter is identified. When employees reveal organizational wrongdoing using their real name (providing information that recognizes the individual employee personally), it is referred to as identified whistleblowing. Conversely, when employees report organizational wrongdoing by hiding their identity, it is referred to as anonymous whistleblowing. Empirical research (e.g. Kaplan and Schultz 2007;

Robinson, Robertson and Curtis 2012) suggest that when employees use anonymous whistleblowing, the reporting of organizational misconducts, such as, fraud and corruption increases since the perceived personal cost of blowing the whistle decreases for the whistle-blower. Anonymous reporting, therefore, enhances the effectiveness of whistleblowing to discern and expose corporate wrongdoing. However, while blowing the whistle anonymously tends to make the disclosure easier for the whistle-blower, it can create difficulties in the investigation of the report if the organization does not have designated procedures where confidentiality and anonymity are maintained as part of the organization's response to managing the report and putting an end to the reported wrongdoing.

Organizational Response to Managing, Addressing, and Ending Corporate Wrongdoing

The organization and its members need to share a firm conviction that the tolerance of illegal and unethical behaviour is not in their own, or the organization's interests, and that the eradication of corporate wrongdoing must become internalized. Organizations must therefore implement an effective internal system for employees to raise concerns and to facilitate the process of whistle-blowing internally. If individuals feel that it is not safe and accepted to blow the whistle internally, they will resolve to blow the whistle externally. Management must further demonstrate a commitment to investigate all allegations promptly and thoroughly, and report the origins and the results of the investigation to a higher authority. Too often, the reporting channels are not trusted, and observers of wrongdoing are uncertain of the organizational agent to make reports. Within both case studies in the healthcare industry, unfavourable organizational responses, or rather, no responses to observed and reported wrongdoing transpired subsequent to reporting.

It is apparent that within organizational responses to corporate wrongdoing, three parties are important: the individual(s) who commits the (alleged) wrongdoing, the observer who considers the act wrong and reports it, and the recipient of the whistle-blower's report. When developing and implementing whistleblowing policies all parties must be covered. The implementation of whistleblowing policies are increasingly being recommended by many codes of corporate governance as well. At a minimum, an effective internal policy on whistle-blowing should include: a clear statement that malpractices are taken seriously, confidentiality is respected, that there are penalties for false and malicious allegations, and a clear indication of how the concern can be raised internally and as a last resort, externally if necessary. The internal system should also include proper communication channels, commitment by management to the whistle-blowing process and support approaches for the whistle-blower. Since corporate governance is fundamental to effective management within an organization, this means whistleblowing policies can be part of internal auditors' responsibilities as well. In 2014, the Securities Exchange Commission (SEC) announced a whistle-blower award of more than \$300,000 to a company employee who performed audit and compliance functions. This employee reported wrongdoing to the SEC after the company failed to take action when the wrongdoing was reported it internally. Indeed, individuals who perform internal audit, compliance, and legal functions for companies are on the front lines in the battle against fraud and corruption. They often are privy to the very kinds of specific, timely, and credible information that can prevent an imminent fraud or stop an on-going one. Managerial frameworks on whistleblowing should therefore, incorporate the role of internal audits and audit committees. The use of financial rewards however, should be closely monitored to prevent possible abuse of the system for personal gains.

Organizational Response to Whistle-Blower

To blow the whistle is not an easy task, it needs courage, moral evaluation, and one has to put the interest of the public ahead of his or her interest. Despite this, many praise whistle-blowers for heroic and noble deeds; many also condemn them as malcontent, trouble makers and misfits for exposing misfeasance and wrongdoing of their colleagues and management. The whistle-blower can be viewed positively, or negatively, regardless of whether the whistle has been blown through internal channels or, as a last resort, through external channels. The response of the organization to the whistle-blower, whether positive or negative, largely depends upon the style and approach of top management.

Organizations need to create an environment where employees can feel safe as whistle-blowers and where they are encouraged to report wrongdoing knowing that they will be protected and that the wrongdoing will be addressed. In this regard, top management support largely shapes this environment and hence the organizational response to the whistle-blower. As organizational policy-makers, top managers must consider the whistle-blower objectively. It is not an issue that can be ignored, due to the possible negative consequences for the whistle-blower, other employees and the organization. Managers should therefore, be supportive of employees who may have a problem as an observer of corporate wrongdoing right through to the management of the issue and the organizational life of the whistle-blower after the issue is addressed.

Like most initiatives, a whistle-blower program is most effective when supported by the organization's leadership. If the company has cohesive whistle-blower and ethics policies – and if both are adhered to by management – then individuals will be more willing to report suspicious activities. A senior-level “hotline champion” who owns and oversees the program also reinforces its significance. The champion should be someone with authority to make decisions and act on tips; if the organization has an Ethics or Compliance Officer, that individual should be an ideal candidate.

SOLUTIONS AND RECOMMENDATIONS

From a managerial perspective, it must be recognized that the key aspects of any whistleblowing framework would be incomplete in the absence of supporting whistleblowing legislation and a supportive culture.

The Role of Whistleblowing Legislation

Within any management framework for whistleblowing, whistleblowing legislation is critically important for its effectiveness in identifying, reporting, managing, and rooting out corporate wrongdoing, while protecting the welfare and interests of the whistle-blower. Globally, across both the private and public sectors, whistleblowing policies to protect the organization, the whistle-blower, and to address organizational misconduct have undeniably been promoted as key aspects of the management of whistleblowing. Whistleblowing policies are relevant and can play a critical role in implementing management practices, which is a key ingredient of organizational growth. For example, in the United Kingdom, the Combined Code on Corporate Governance promotes the revision of arrangements by audit committees as it relates how employees can confidentially raise concerns about possible improprieties in matters of financial reporting or other matters, and to ensure that independent and proportionate investigative

arrangements are organized and the relevant follow up actions are undertaken. In the United States, the Sarbanes-Oxley Act, which provides guidelines for the operation and management of public companies, also highlights the enhanced responsibilities of external auditors, audit committees, board of directors and effective whistle-blowing mechanisms, for the protection of stakeholders and the public's interest.

Such whistleblowing policies have been shown to be much more effective however, in the presence of a specific and detailed whistleblowing legislative framework. To supplement the existing reporting mechanisms, there needs to be more protection for whistle-blowers in society and organizations, especially in an environment where there are high personal costs for reporting. This protection can come in the form of whistle-blower legislation which can incentivize whistleblowing and penalize wrongdoers and persons who obstruct whistle-blowers. The SEC's Whistle-blower Award is an example of the incentivizing of whistleblowing. In response, several countries globally have recognized the need to support and extend organizational whistleblowing policies through specific whistleblowing legislation. Most recently, on April 23, 2018, the European Union (EU) drafted a new law designed to strengthen the protections given to whistle-blowers across the bloc.

Other Examples of Whistleblowing Legislation

- United Kingdom Public Interest Disclosures Act, 1998
- Securities Exchange Commission (SEC) Whistleblowing Program, 2010
- Japan Whistle-blower Protection Act, 1994
- South Korea Anti-corruption and Protection Act, 2001
- New Zealand Public Service Whistle-blowing Act, 2000
- Whistle-blowers Protection Act in Australia (Victoria), 2001
- Protected Disclosures Act in Jamaica, 2011

Within such Acts, provisions are also made for a code of conduct, the protection of the whistle-blower, whistleblowing channels, procedures and support structures for, and programmes to promote whistleblowing. In the U.S and Australia, for instance, annual reports must be released specifying the current guidelines, the number of disclosures investigated and referred to other public agencies. In the U.S, as well, toll-free helplines have been opened for employees of private and public companies to report suspected misconduct or fraud. Notably, when whistleblowing policies are supported by whistleblowing legislation, not only a moral obligation, but a legal obligation is created to blow the whistle on corporate wrongdoing. Further, it promotes an environment of safety for whistleblowing within the ambits of the law.

Even in the face of such legislative frameworks, protection within the management of whistleblowing still needs work. For example, Hervé Falciani, a whistle-blower who leaked documents alleging widespread tax evasion at HSBC's private banking arm, has faced extradition requests from Swiss authorities. Howard Wilkinson, the former Danske Bank manager who alleged the bank was caught up in a €200bn money laundering scheme, called upon national governments to offer him greater protection after his identity was disclosed. Clearly, the safeguards in place to defend whistle-blowers against reprisals are insufficient. It is therefore, apparent that the majority of people around the world, speaking up about cases of wrongdoing in the workplace are perilous, and legal protection is insufficient even in the face of disclosure legislation. Many citizens still remain largely unprotected if they speak up, facing the risk of retaliation, judicial proceedings and dismissal. Such cases are further complicated where legal and ethical conflicts emerge in relation to whistleblowing.

The problem is that the protection afforded to whistle-blowers varies country by country and legal and ethical conflicts further complicate whistleblowing legislation. For example, in some nations such as the United Arab Emirates (UAE), whistleblowing legislation conflicts with defamation clauses in the country's penal code, and with the code of conduct and ethics of many organizations. Whistleblowing is not clearly defined by UAE law. In terms of the obligation to report wrongdoing, the UAE Penal Code contains a requirement that all individuals in the UAE report criminal activity. However, in practice, this requirement is not rigorously enforced and it also fails to address unethical practices or go on to provide protection from retaliation for those who report criminal activity. Accordingly, whistleblowing has traditionally been a less common practice in the UAE than in other developed jurisdictions, particularly in the U.S where whistle-blowers are not just protected but, in many cases, are incentivized to make disclosures.

It is therefore important that such legal and ethical conflicts are addressed within the management of whistleblowing. To do so, it is recommended that complementary codes of organizational ethics be established and aligned to universal legal frameworks to further minimize the need for external whistleblowing as well. There is the need for a unified global stance on the need for whistleblowing, the procedures to be followed for enforcement, and protection for all parties involved from an organizational and legal perspective. In Australia for example, whistleblowing protection laws in its final stages include fines for organizations that do not have whistleblowing policies and requires whistle-blowers to have objective grounds, not just "good faith" for so doing. Universal legislation alone therefore is insufficient and must function within organizational frameworks that promote organizational ethics.

The Role of Culture in Whistleblowing

In addition to a supportive legislative framework for whistleblowing and the promotion of organizational ethics, cultural factors can also play an important role in the acceptance and adoption of whistleblowing within particular organizations and societies. Organizational and national cultures determine how individuals perceive whistleblowing, but it also impacts how whistle-blowers are viewed and treated.

Organizational culture has been commonly defined as shared values, beliefs and assumptions among employees within an organization. Values and beliefs develop and evolve through the constant negotiation and practices among employees in an organization. These values and beliefs develop through time and provide a foundation for what is thought appropriate or inappropriate in a company with regards to right and wrong behaviour. Organizational culture therefore reflects the dominant ideology that exists within individuals' mind, conveys a sense of identity to workers and gives the unwritten and unspoken rules that instruct them on how to get along in their workplace. The organizational culture must be shaped to communicate to staff that whistle-blowing is accepted and unethical conduct will not be tolerated. Effective whistleblowing arrangements are an important part of a healthy corporate culture. But it is also crucial to have the right organizational culture which encourages people to speak out without fear. If the culture encourages principles of good corporate governance and shuns any form of organizational misconduct, an ethical climate can emerge. Further, if the organizational culture is open to, supports, and protects whistle-blowers, whistleblowing approaches and policies are likely to be much more effective in managing and rooting out corporate wrongdoing in such organizations. National culture frameworks such as Hofstede's Culture Consequences (1980) also acknowledge that across different societies and

countries, cultural norms and values can also impact upon the acceptance and success of whistleblowing. For instance, in collectivistic societies such as China, Hong Kong, Taiwan and various Caribbean countries, individuals are more inclined to act in accordance with the norms and interests of 'in-groups'. It is therefore expected that conflicts and face-to-face confrontations may be kept at a minimum. In this regard, it may be difficult for boards and shareholders to effectively function in their respective positions, given the conflict of interests that can arise as a result of close relationships formed in such societies. This suggests that employees in these particular societies may be reluctant to blow the whistle when the need arises. Scepticism may also exist about the reality of whistle-blowers' protection in these countries, even in the presence of a supportive legislative framework. It is imperative that organizations take into account such national culture differences across countries when developing and using whistleblowing mechanisms, such as whistleblowing processes, policies and legislative frameworks since such cultural differences can impact the relevance and usefulness of whistleblowing.

Other Recommendations to Manage Corporate Wrongdoing

Whistleblowing must also be managed within the context of other employee strategies aimed at enhancing employment relationships. Human resource management (HRM) practices such as recruitment and selection, as well as, training and rewards should be used as functions to support and complement whistleblowing mechanisms. Indeed, such HR practices should set the context for employment relationships in recognizing that corporate wrongdoing in the first instance should not be tolerated as a precursor to the management of whistleblowing.

Recruitment and Selection

Organizations, both private and public, should consider the ethical predisposition and ethical sensitivity of applicants in the hiring process so as to minimize tolerance of and actual corporate wrongdoing. More specifically, personality tests and integrity tests can be incorporated as part of the selection criterion for new employees. This initiative at the start of employment relationships can assist in creating an ethical environment, which can only lead to the enhancement of the organization's image and reputation in the long run.

Training and Rewards

Organizations can provide training and development opportunities focused on the resolution of moral issues, the implementation of company policies on ethics and the reporting of wrongdoing, and the institution of reward systems for ethical and reporting behaviours. Such training and reward opportunities can create an environment where organizational misconduct is minimized. It should be noted that the public interest is generally served when ethical behaviour is followed. Conversely, the failure to follow ethical behaviour can have negative implications for organizations and society. Organizations should therefore also develop and institute ethics committees responsible for ensuring that misconduct is reported and managed, while training employees on how to address ethical dilemmas within the committees and rewarding them accordingly.

FUTURE RESEARCH DIRECTIONS

The term whistleblowing is thought to have its roots in the act of police officers and referees blowing their whistle to halt suspected criminals and to stop an action respectively. In the corporate context today, whistleblowing has emerged as a powerful disclosure mechanism for identifying, exposing, managing and rooting out corporate misconduct.

Indeed, unethical and illegal corporate activities continue to plague societies. In future, it is expected that such activities will increase if left unchecked and unmanaged, with even more devastating effects than experienced in the last few decades. As such, there is an even more powerful role for whistleblowing in the future as white-collar crime continues to increase. There is a need however for all organizations to recognize that they must open up to scrutiny and disclosure. For too long, there has been limited recognition that managerial frameworks must be adopted to maximize the benefits of whistleblowing.

Future research, building from this work, should explore the symmetry between corporate wrongdoing or corporate misconduct and other criminal activities. Indeed, there may be spill-over effects from corporate wrongdoing into other areas of crime. This spill-over has the potential to exponentially increase crime and criminal activities beyond the boundaries of the organization. If so, such future research will reinforce the need for all organizations to embrace and maximize whistleblowing given its power to manage corporate wrongdoing.

CONCLUSION

Whistleblowing can provide the basis for managing, addressing, and preventing corporate wrongdoing and misconduct as a disclosure mechanism. Whistleblowing can not only help to reduce white-collar crime but can also prevent the collapse of organizations under the weight of fraud, corruption, and other forms of misconduct, which can lead to corporate bankruptcy as well. Even so, not many observers of corporate misconduct are willing to come forward and blow the whistle. This is partly due to the possibility of severe reprisal on the whistle-blowers by their peers and employers as a result of incriminating information on their employers. In spite of the high personal costs of whistleblowing on the whistle-blower, it is undeniable that a structured management approach must be taken to maximize the benefits of whistleblowing in addressing corporate wrongdoing, while also addressing the concerns of whistle-blowers.

A structured management framework must take into account procedures for identifying acts which constitute corporate wrongdoing or misconduct, reporting structures for the wrongdoing, the organizational response to managing, addressing and ending the wrongful acts revealed through reporting, and the organizational response to the whistle-blower. Such a framework must also take into account the relevance of whistleblowing legislation, the role of culture in enhancing the effectiveness of whistleblowing, and the impact of supportive HRM functions in establishing an ethical climate where organizational misconduct is discouraged.

Even so, no standard whistleblowing framework with supporting mechanisms may work for all organizations in the same way. However, it can provide the foundation for recognizing the power of whistleblowing in rooting out corporate wrongdoing.

REFERENCES

- Berry, B. (2004). Organizational Culture: A Framework and Strategies for Facilitating Employee Whistleblowing. *Employee Responsibilities and Rights Journal*, 16(1), 1–11. doi:10.1023/B:ERRJ.0000017516.40437.b1
- De George, R. T. (1986). Whistleblowing. In *Business Ethics* (pp. 221–238). New York: Macmillan Publishing Company.
- Dungan, J., Waytz, A., & Young, L. (2015). The psychology of whistleblowing. *Current Opinion in Psychology*, 6, 129–133. doi:10.1016/j.copsyc.2015.07.005
- Fletcher, J. J., Sorrell, M., & Silva, M. C. (1998). Whistleblowing as a failure of organizational ethics. *Online Journal of Issues in Nursing*, 3(3), 1–15.
- Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-related Values*. Beverly Hills, CA: Sage Publishers.
- Kaplan, S. E. Jr, & Schultz, J. Jr. (2007). Intentions to report questionable acts: An examination of the influence of an anonymous reporting channel, internal audit quality and setting. *Journal of Business Ethics*, 71(2), 109–124. doi:10.1007/10551-006-0021-6
- Kaptein, M. (2011). From Inaction to External Whistleblowing: The Influence of the Ethical Culture of Organizations on Employee Responses to Observed Wrongdoing. *Journal of Business Ethics*, 98(3), 513–530. doi:10.1007/10551-010-0591-1
- Near, J. P., & Miceli, M. P. (1986). Retaliation against whistle blowers: Predictors and effects. *The Journal of Applied Psychology*, 71(1), 137–145. doi:10.1037/0021-9010.71.1.137
- Near, J. P., & Miceli, M. P. (1996). Whistle-blowing: Myth and reality. *Journal of Management*, 22(3), 507–526. doi:10.1177/014920639602200306
- Ray, S. (2006). Whistleblowing and Organizational Ethics. *Nursing Ethics*, 13(4), 438–445. doi:10.1191/0969733006ne882oa PMID:16838574
- Robinson, S. N., Robertson, J. C., & Curtis, M. B. (2012). The effects of contextual and wrongdoing attributes on organizational employees' whistleblowing intentions following fraud. *Journal of Business Ethics*, 106(2), 213–227. doi:10.1007/10551-011-0990-y

ADDITIONAL READING

- Dozier, J. B., & Miceli, M. P. (1985). Potential predictors of whistle-blowing: A prosocial behaviour perspective. *Academy of Management Review*, 10(4), 823–836. doi:10.5465/amr.1985.4279105
- Felli, L., & Hortala-Vallve, R. (2016). Collusion, blackmail and whistle-Blowing. *Quarterly Journal of Political Science*, 11(3), 279–312. doi:10.1561/100.00015060
- Figg, J. (2000). Whistleblowing. *Internal Auditor*, 57(2), 30.

Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008). *Whistle-blowing in Organisations*. New York, NY: Taylor & Francis.

Rachagan, S., & Kuppusamy, K. (2012). Encouraging whistle blowing to improve corporate governance? A Malaysian initiative. *Journal of Business Ethics*, 115(2), 367–382. doi:10.1007/10551-012-1402-7

Schein, E. (2016). Whistle Blowing: A Message to Leaders and Managers, Comment on Cultures of Silence and Cultures of Voice: The Role of Whistleblowing in Healthcare Organizations. *International Journal of Health Policy and Management*, 5(4), 265–266. doi:10.15171/ijhpm.2015.207 PMID:27239866

KEY TERMS AND DEFINITIONS

Disclosure: The process of revealing something.

Enron: A company in the United States which went bankrupt in 2001 due to accounting fraud. It has been dubbed the worst accounting scandal in history, and it was exposed through whistleblowing.

HRM: Acronym for human resource management. A set of practices to attract, develop, and maintain an effective workforce.

Illegal: Actions or practices which are against the law.

Unethical: Actions or practices deemed immoral or wrong.

Whistleblower: An individual who reveals wrongdoing to some higher authority. Illegal and unethical activities are usually revealed by such a person.

Whistleblowing: The act of revealing wrongdoing to some higher authority. Illegal and unethical activities are using revealed.

Whistleblowing to Expose Criminal Activity in the Health Sector

Niyi Awofeso

School of Health and Environmental Studies, Hamdan Bin Mohammed Smart University, UAE

INTRODUCTION

Whistleblowing is the non-obligatory act of disclosing information about unethical or criminal activity in an organization. Although most instances of whistleblowing in the health sector relate to patient safety issues such as reporting on poor clinical outcomes involving a single individual over a period (Dyer, 2005; Bolsin et al, 2011), the health sector is not immune from criminal activity. Health care fraud – defined as an intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party - is a major crime in most nations, accounting for 2% to 10% of total healthcare costs. In countries with universal health insurance such as UAE, health insurance fraud may account for up to 10% of total health insurance claims (Awofeso, 2017). The World Health Organization has cited fraud as one of 10 leading causes of inefficiency in health systems (WHO, 2010). The current global average loss rate of 6.19% attributable to health system fraud expressed as a proportion of 2013 global health budget of \$7.35 trillion equates to \$455 billion (Gee and Button, 2015).

In most other nations, (external) whistleblowing – leaking information to the press or independent healthcare complaints boards, for example, is discouraged due to reputational effects on the organization. Pertinent in this regard is the impact of vexatious whistleblowing, in which whistleblowers may accuse healthcare personnel of, for example, research fraud, without substantiating their claims – leading to incalculable damage to professional and organisational reputation (Wright, 2010). There is also a somewhat paternalistic reason why some organizations appear to discourage (external) whistleblowing – whistleblowers suffer substantial ostracization from colleagues and senior management, even if the whistleblower's accounts are true. (van de Verden et al, 2018). Whistleblowing situations are stressful and may cause physical and emotional health problems for both whistleblowers and non-whistleblowers (McDonald & Ahern, 2002).

Over the past three decades since the World Wide Web became established internationally, it has produced mixed results for both facilitating and preventing criminal activity in the health sector. With the expansion in online use of health care in payments, data storage and medical devices using online platforms, the risks to patient data confidentiality and cyberattacks on medical devices have increased exponentially. Since 2000, the American Medical Association has deemed internet healthcare ethics an important sector, and implemented principles governing websites that its members use for health related purposes, such as; “*Medical websites, more than any other type of site on the Internet, should ensure visitors' personal privacy and prevent personal medical information, including patterns of use and interests, from being sold, purchased, or inadvertently entering the hands of marketers, employers, and insurers.*” (Winker, Flanagi, Chi-lum et al, 2000). With internet technology being increasingly used in health care medical devices as well as in health care research, risks related to hacking of medical

DOI: 10.4018/978-1-5225-9715-5.ch021

devices and falsification of research data may increase. According to the 2018 Stericycle Recall Index report, there was a 126% increase in recalls of medical devices such as cardiac pacemakers between 2017 and 2018, mainly due to software hacking vulnerabilities (Stericycle Expert solutions, 2018). The use of internet-based media outlets enables whistleblower activities to reach every corner of the globe, with major adverse consequences for the organization and the whistleblower. These issues illustrate the nexus between healthcare, the internet and illegal or unethical activities.

Background

The role of the whistleblower in detecting healthcare fraud is perceived as important in some industrialized nations such as the United States, Australia and United Kingdom. For example, in the United States, Medicare processes over one billion fee-for-service claims per year through its contracts with regional insurance companies. Given the enormous volume of claims submitted under the Medicare program, the federal and state governments are not sufficiently staffed to effectively detect the fraud and abuse perpetrated by dishonest physicians, healthcare providers and suppliers. The Whistleblower Protection Act was made into federal law in the United States in 1989. The US Securities and Exchange Commission (SEC) has awarded more than \$262 million to 53 whistleblowers since issuing its first award in 2012. All payments are made out of an investor protection fund established by Congress that is financed entirely through monetary sanctions paid to the SEC by securities law violators.

Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action. Whistleblower awards can range from 10 percent to 30 percent of the money collected when the monetary sanctions exceed \$1 million. In December 2017, Australia introduced The Treasury Laws Amendment (Whistleblowers) Bill 2017, which introduces a specific whistleblower protection and compensation regime for those who expose misconduct in public health and safety, tax and corporate fraud affairs. Public companies and large private companies that fail to set up internal whistleblower policies before 1 January 2019 risk facing penalties of up to 60 penalty units (currently A\$63,000 for a body corporate).

It is helpful to distinguish between internal whistleblowing, which entails employees reporting criminal or patient safety concerns to managers internal to their organization, from classic (external) whistleblowing, when an employee reveals information externally (or publicly) about wrongdoing within the organization, due to the ethical and consequential differences between both variants of whistleblowing. External Whistleblowers often end up choosing between failing in a duty to the public and failing in a duty to their employer, and they chose to fail in their duty to their employer, irrespective of whether the employer has a legitimate or moral standing in the issue concerned. Such violation of the *pro tanto* obligation to the employer impairs the moral standing of whistleblowers (MacDougall, 2016).

Ethical and Legal Aspects of Whistleblowing in Health Sector

Health care ethics is the field of applied ethics that is concerned with the vast array of moral decision-making situations that arise in the delivery of health services. Essential to the comprehension of moral issues that arise in the context of the provision of health care is an understanding of the most important ethical principles and methods of moral decision-making that are applicable to such moral issues. There are several core ethical approaches to understand whistleblowing in the health sector – utilitarian ethics, virtue ethics, organizational ethics, and deontological ethics. Utilitarianism is a variant of rule conse-

quentialist ethics, which posits that the morally right action is one with the best overall consequences. Whistle blowing may be supported by utilitarianism if it will benefit a significant number of people. A hedonic calculus may be applied to evaluate the harms and benefits of whistleblowing, but this approach is likely to underestimate the harms given that whistleblowing settings tend to affect an overwhelming majority of individuals in such settings. Internal whistleblowing reduces the harms caused by exposing misconduct (Wilmot, 2000).

Virtue ethics is one of three major approaches in normative ethics. It may be described as an approach that emphasizes techniques promoting an agent's character and instructing their conscience, may motivate whistleblowing particularly among individuals with a dominant (benevolent) superego (Nair, 2002). Integrity is a virtue that aligns with motivations to report wrongdoing. Most healthcare professionals code of ethics and conduct include the value of integrity. Thus, reluctance to engage in whistleblowing when there are compelling reasons to do so may violate the integrity virtue. Ironically, loyalty to organizations is one of the conditions of employment in many health organizations, and external whistleblowing may violate such employment condition, expressed as betrayal of trust (Pellegrino, 1995; CNA 1999).

Organization ethics includes various guidelines and principles which decide the way individuals should behave at the workplace. Fiduciary relationships (i.e. relational ethics) are integral to organizational ethics as they underscore loyalty, integrity and organizational structures. Fiduciary relationships exist between employer and employee, as well as between healthcare providers and patients. A conflict of loyalty usually implies a failure of organizational ethics and accountability since, under normal circumstances, both fiduciary relationships should be well aligned. Healthcare organizations that do not support whistleblowers reporting fraud or violations of professional standards suffer from a failure of organizational ethics. (Fletcher, Sorrell and Silvia, 1998; Ray, 2006).

Deontology is a variant of normative theories regarding which choices are morally required, forbidden, or permitted. It guides and assesses our choices of what we ought to do, and posits that the morality of an action should be based on whether that action itself is right or wrong under a series of rules, rather than based on the consequences of the action. Whistleblowers who align with a deontological approach view the act as a duty that needs to be undertaken as part of their moral and professional obligations, irrespective of its consequences. External whistleblowing in the health sector regarding criminal, fraudulent or patient safety grounds prioritizes loyalty duties to patients over and above loyalty to implicated colleagues or the organization as a whole. However, deontology is related to moral rules, not legal ones. In line with studies in other sectors (Keenan, 2000), deontological rules significantly motivate whistleblowing in healthcare settings.

The high profile media attention which whistleblowing has attracted across the world in recent years has underlined its relevance to all organizations. For instance, in 2013, an anonymous whistleblower sent an email to British pharmaceutical company GlaxoSmithKline (GSK) board members, external auditor, Chinese government and senior executives, describing fraudulent activities in China. The whistleblower stated that medical professionals were given all-expenses-paid trips under the pretense of attending professional conferences. Also, that the drug Lamictal was being heavily promoted as a treatment for bipolar disorder, despite being approved only for treatment of epilepsy by Chinese regulators. Bribes totaling \$9000 were allegedly paid to a patients who experienced adverse reactions to Lamictal in order to keep the patient's silence. In 2014, the company was fined \$489 million by Chinese courts for bribing doctors and hospitals to use its products and bribing government officials and regulators to ease monitoring of GSK. It is not clear what motivated the anonymous whistle blower, and whether he received any pecuniary benefit, or sanctions, for his actions.

In many nations in which whistleblowing is essentially a criminal activity, the internet has served as a vital vehicle for achieving the whistleblowers' aims. The legal system's general hesitancy to extend protection to media whistleblowers is reinforced by the perception that reporters and online internet sites are used by less "worthy" whistleblowers - those with groundless claims, those who are vengeful, and those with other ignoble motives (Callahan and Dworkin, 1994).

In the United States, The Securities and Exchange Commission won new powers in the 2010 Dodd-Frank Wall Street reform law to entice whistleblowers with monetary awards. A record \$30 million was paid to an anonymous whistleblower for helping to uncover large-scale fraud, essentially 10 – 30% of total amount recovered by the US government (Rickman, 2017). Among G20 nations, whistleblower protection laws are most explicit in USA, UK, Japan, and China but are less so in Germany and France. Australia's explicit whistleblowing protection law is currently undergoing deliberations in its parliament. Only USA, Japan and China explicitly provide protections for external whistleblowers. In the Middle East region, Bahrain has the most restrictive whistleblower laws. In the United Arab Emirates, whistleblowing is not currently protected at a federal level and in certain circumstances whistleblowing may potentially lead to both criminal and civil liability for breach of confidentiality and criminal liability for defamation. However, in Dubai, Dubai Law 4/2016 on Financial Crimes has some modest protections for whistleblowers in respect of certain financial crimes. The mapping of whistleblowing legislation for selected countries is shown below in Figure 1 (Piper, 2015).

Whistleblowing and Patient Safety Violations

Patient safety is essentially about policies, procedures and practices that guarantee the prevention of harm to patients - those that reduce the risk of adverse events related to exposure to medical care across a range of diagnoses or conditions (Clancy, Farquhar & Sharp, 2005). In the context of patient safety, whistleblowing commonly entails identifying incompetent, unethical or illegal situation in the workplace, and reporting it to someone who may have the authority to stop the misdeed. Often 'whistleblowing' is used as a term when a concern feels unwelcome or when it's external, and 'freedom to speak up' or 'raising concern' are seen as being at the softer end of the spectrum, when a staff member first identifies and reports incompetent practices which may or may not be illegal. In most countries, laws determine whether breaches in patient safety can have legal consequences for individuals and institutions. Major patient safety breaches fall under the category of tort, or personal injury. Negligence as a tort is the breach of the legal duty to take care which result in damage, undesired by the defendant, to the plaintiff. Tort law seeks to compensate victims of certain actions or inactions based on the breach of a legal duty that caused damages (Ramanathan, 2014).

Two interesting Australian cases of whistleblowing in relation to patient safety concerns occurred in the Macarthur Health Service in New South Wales and Bundaberg Base Hospital in Queensland. The nurse whistleblowing in both cases occurred consequent to dysfunctional clinical governance and incident reporting processes. The Macarthur health service is located in South-West Sydney, and incorporates Camden hospital, Campbelltown hospital and Queen Victoria memorial nursing home. On 5 November 2012, four employee nurses of the health service met with the state health minister, and reported cases of substandard clinical practices resulting in patient deaths and injuries. These nurses have previously utilized internal reporting systems such as incident reports, reports to line managers or referral of cases to relevant peer-review committees. However, they felt that their efforts were both unwelcome and ineffective in changing the health services' unsatisfactory patient safety trends. Even reports sent to the senior executive level of the health service as well as the New South Wales nurses association

Figure 1. Whistleblowing protection ratings across the globe

Note: Little or no protection - *; Some protection through general laws - **, Express protection - ***

EUROPE	
Austria	★★
Belgium	★
France	★★
Germany	★★
Hungary	★★
Italy	★★
Netherlands	★★
Norway	★★
Poland	★★
Spain	★★
Romania	★
Sweden	★★
Turkey	★★
United Kingdom	★★★
AMERICAS	
Brazil	★
Mexico	★★
US	★★★
AFRICA	
South Africa	★★★
ASIA-PACIFIC	
Australia	★★
China	★★★
Hong Kong	★
Japan	★★★
South Korea	★★★
India	★
Indonesia	★
Malaysia	★★
Singapore	★
Thailand	★★
MIDDLE EAST	
UAE	★★
Kingdom of Saudi Arabia	★★
Qatar	★★
Bahrain	★
Kuwait	★★

were forwarded to the hospital middle management to investigate. The minister referred the case to the State's Health Care Complaints Commission (HCCC) to formally investigate. The investigation resulted in an analysis of 47 clinical incidents alleged to have occurred between June 1999 and February 2003. After 13 months of investigation, the HCCC report was delivered to the Director general of the health Department in December 2003. The published report strongly supported most of the allegations made by the nurses, e.g. "in some instances the care was so poor that patients suffered serious deterioration in health" (HCCC 2003, p4, part 1). In spite of these adverse findings, no prosecution or disciplinary action was recommended against those found to have breached their duties of care. The new health minister, Mr. Morris Iemma, decided to sack both the HCCC board and the then HCCC commissioner, Ms. Amanda Adrian. In all, there were five major inquiries costing many millions of dollars, and the devastation of scores of careers. At the end of it all, there have been big changes and more money for

the Macarthur Health Service. Yet only eight doctors faced disciplinary action. The outcome of the first case to go to the Medical Tribunal was announced this week. The doctor was reprimanded, but the judge said “his failure to act was in no way a gross dereliction of duty. In those circumstances it is somewhat surprising that a complaint was made to bring him before the Medical Tribunal.” In September 2015, the New South Wales Independent Commission Against Corruption produced the second of two reports into claims made by the four whistleblower nurses. It found that not one of the 39 serious allegations was substantiated. All four whistleblower nurses resigned from the Campbelltown hospital within two years. They reported adverse emotional consequences directly related to the case. According to one of them – Nola Fraser – “The personal effect was devastating: I couldn’t sleep for two years; I cried myself to sleep to think that those patients could have been saved if somebody just cared”. In late 2001 she went into intense therapy for 12 months. In March 2002, after yet another fight with her superiors, she walked out and went on extended sick leave due to depression and stress. As for Fraser’s former colleagues, most of whom won’t speak on the record, they are bitterly resentful. There are many stories of lives disrupted and long periods of depression. One said: “You’d think being investigated would be OK if you’re innocent. But it’s not. It’s traumatic.” By making many claims that were later proved to be wrong, the whistleblower nurses caused many people anguish. Nevertheless, they highlighted problems that deserve to be better known.

The Bundaberg Base hospital whistleblowing episode revolved around an Indian-born American surgeon, Jayant Patel, who was found guilty of gross negligence in 2005 whilst working at the 136-bed Bundaberg Base Hospital in a remote region of Queensland, Australia. Dr. previously worked with the renowned Kaiser Permanente hospital in Portland, USA. In his application to practice surgery at Bundaberg base Hospital, Dr. Patel fraudulently answered “No” to all application questions related to history of suspension or cancellation of his medical registration. Yet, the New York medical board for professional conduct suspended his license for 6 months and placed him on 3-year probation for entering patients’ histories and physical findings without actually examining patients, failing to maintain patients’ records, gross negligence, and harassing patients who were cooperating with the New York Board’s investigation (Bundaberg Hospital CoI Report, 2005). Patel was employed at the Bundaberg hospital between 2003 and 2005, during which he operated on about 1000 patients and performed about 400 endoscopic procedures. Nurses working with Dr. Patel repeatedly complained through internal channels such as occurrence variance reports about his sub-optimal level of surgical competence and associated high post-operative complications. Nurse Toni Hoffman formally complained about Dr. Patel to Bundaberg hospital directors of nursing and medical services in 2003 when he performed a complex operation – oesophagectomy – on two patients (P18 and P34) – although the ICU at the hospital was not equipped to provide artificial ventilation for more than 48 hours. Patient 34 died a few hours following surgery, while patient 18 suffered serious complications. After about a dozen other adverse clinical incidents involving Dr. Patel, an external clinical audit review was commenced at Bundaberg hospital in January 2005.

However, evidence for investigating the scope of practice and quality of Dr. Patel’s surgical outcomes were not initially collected. He even had his contract “temporarily” extended from 2005 to 2009. Following multiple ignored internal reports, Toni Hoffman decided to report Dr. Patel to Mr. Rob Messenger, local member of the Queensland Parliament, seat of Burnett. At the meeting with Mr. Messenger on 18 March 2005, Hoffman requested whistleblower status and expressed a desire to remain anonymous. On 22 March 2005, Mr. Messenger tabled Ms. Hoffman’s complaint at the Queensland parliament, leading to the implementation of two inquiries into Dr. Patel and Queensland hospital starting 26 April 2005. The health systems review highlighted a failure of organizational ethics in the Queensland health system, with strong themes highlighting bullying, intimidation, blaming and avoiding responsibility (Forster, 2005).

The Bundaberg hospital Commission of Inquiry (2005) was initially terminated on 2 September 2005 following a reasonable apprehension of bias against inquiry commissioner Morris. Following public pressure instigated by whistleblower Toni Hoffman, the inquiry was reinstated and a new commissioner, Geoff Davies was appointed. The inquiry castigated Bundaberg hospital management for failure to properly check Dr. Patel's background, and failure of credible incident reporting and complaints system. Commissioner Davies detailed nine specific charges against Dr. Patel, including performing surgical procedures restricted by previous medical boards and failure to report 13 deaths to the coroner. Davies recommended Dr. Patel to be investigated by Queensland police for "fraud", "negligent acts causing harm" and "manslaughter". Patel was extradited from the US to Australia and was convicted and jailed on all 3 counts. After two years of imprisonment, Patel was granted bail in 2012 after it was concluded that his trial was tainted by highly emotive and prejudicial evidence. In November 2013, Patel was given a two-year suspended sentence.

The head of a royal commission-style inquiry, former Supreme Court judge Geoff Davies, lauded Toni Hoffman as a hero in late 2005. He found her care, passion and courage were key in bringing to light a disaster, that led to at least 13 deaths and injuries to dozens of patients. At a personal level however, Toni Hoffman lamented that her career, health and psychiatric wellbeing were now severely affected because bureaucrats and successive ministers caused her to be increasingly shunned and ostracized. She claimed that she is being portrayed by Queensland Health and its corporate chiefs as "the untrustworthy nurse who embarrassed us all". Although she received the Order of Australia medal and Local Hero recognition in 2006, she claimed that she was threatened with "performance management" and left in no doubt that her career was at a standstill or worse. She eventually negotiated a payout compensation package with Queensland health service.

Whistleblowing and Health Research Ethics Violations

There is no generally agreed definition of research; however, it is widely understood to include at least investigation undertaken to gain knowledge and understanding or to train researchers. Human research is conducted with or about people, or their data or tissue. Human participation in research is therefore to be understood broadly, to include the involvement of human beings through taking part in surveys, interviews or focus groups, undergoing psychological, physiological or medical testing or treatment, being observed by researchers, and researchers having access to their personal documents or other materials. The relationship between researchers and research participants is the ground on which human research is conducted. Important ethical values in research include respect for human beings, research merit and integrity, justice, altruism, respect for cultural diversity and beneficence. These values help to shape that relationship as one of trust, mutual responsibility and ethical equality (NHMRC, 2018).

Research misconduct is defined as fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results. Research misconduct violates research ethics and integrity, and may mislead, harm and discredit the research community and the general public. Among ethics values, respect is central. It involves recognising that each human being has value in himself or herself, and that this value must inform all interaction between people. A classic example of violation of research ethics is the Tuskegee syphilis study among African American males - the longest nontherapeutic experiment on human beings in medical history. Begun in 1932 by the United States Public Health Service (USPHS), the study was purportedly designed to determine the natural course of untreated latent syphilis

in some 400 African American men in Tuskegee, Macon County, Alabama. The research subjects, all of whom had syphilis when they were enrolled in the study were matched against 200 uninfected subjects who served as a control group. The subjects were recruited with misleading promises of “special free treatment,” which were actually spinal taps done without anesthesia to study the neurological effects of syphilis, and they were enrolled without their informed consent. The subjects received heavy metals therapy, standard treatment in 1932, but were denied antibiotic therapy when it became clear in the 1940s that penicillin was a safe and effective treatment for the disease. When penicillin became widely available by the early 1950s as the preferred treatment for syphilis, this therapy was again withheld. On several occasions, the USPHS actually sought to prevent treatment (Heintzelman, 2003).

The project was reluctantly terminated after Peter Buxtun, a former PHS venereal disease investigator, shared the truth about the study’s unethical methods with Associated Press reporter Jean Heller. Congressional hearings into the conduct of the study led to legislation strengthening guidelines to protect human subjects in research (i.e. The Belmont Report). Fred Gray, a civil rights attorney, filed a \$1.8 billion class action lawsuit that resulted in a \$10 million out-of-court settlement for the victims, their families and their heirs. The research was generally adjudged to be so unethical that when in 1997 President Clinton was apologizing for it, he described it as “deeply, profoundly, and morally wrong” (Thomas 2000). Was the action by Buxtun of exposing the malpractices in the Tuskegee Study morally right or wrong? On what grounds do we judge this act of whistle blowing (and the press reporting by Jean Heller) as morally right or wrong? For a Kantian who believes that moral agents have a duty to be morally upright based on the notion of goodwill, such an action could be judged to be morally good (Ogungbure, 2011).

Peer review of research work submitted for publication in scientific journals is a longstanding approach for preventing publication of fraudulent data. However, peer reviewers cannot be expected to detect deliberate and blatant attempts to deceive them. Scientists generally trust that fabrication will be uncovered when other scientists cannot replicate (and therefore validate) finding. However, scientists struggle to replicate and reproduce findings from even highly cited journals. In a landmark article, Stroebe, Postmes, and Spears (2012) highlighted the importance of whistleblowers in uncovering criminal activity in research publications. For 21 of these forty cases they list a “whistle-blower” as the mode of discovery. A further two of the studied cases also entailed whistleblowers: William Summerlin was caught “painting his mice” but it needed the technician who caught him to report this misconduct to prompt Summerlin’s suspension and the formal misconduct inquiry. In the case of Ranjit Chandra, Stroebe and colleagues indicate that journal peer review was a contributor to his unmasking as a data fabricator in 2002. However, a whistle-blower (Marilyn Harvey) had reported him to the Memorial University authorities in 1994 and a subsequent confidential university committee report found him guilty of research fraud. However, no action was taken and he continued to publish fraudulent data for almost another decade.

Rather than being applauded, the experiences of the whistleblowers, as painstakingly documented by Dr. Geoffrey Webb (2018), paint a mixed picture. For example, in 2006, Eric Poehlman was became the first scientist in the USA to receive a prison sentence for activities relating to research fraud. He was convicted by a federal court in Vermont of making a false statement in a US federal grant application and was sentenced to a year and a day in prison. He had previously been fined \$180,000 and banned for life from receiving federal research funding. This case is highlighted because the whistle-blower received a \$22000 share of the \$180000 recovered from Poehlman by the federal authorities. Also Michael Briggs, a Professor at Deakin University, Australia, was unmasked a fraudulent researcher by Dr. James Rossiter, then chair of the ethics committee at Deakin University. Rossiter’s first action was in October 1983 when he reported his suspicions to the chancellor of the university along with a file of supporting

evidence. It was not until 1988 that a final report on the Briggs affair was eventually produced by the university – Briggs resigned from the university in 1985. Rossiter endured several years of intimidation and harassment for his whistleblower activity, but was eventually vindicated in the Deakin university's report (Rossiter, 1992). Also in Australia, the first case of criminal conviction for research fraud occurred in 2016 when Dr. Murdoch and Dr. Barwood of the University of Queensland were convicted on 5 and 17 charges of research fraud and attempted fraud respectively, following the actions of a whistleblower who demonstrated that the data were fabricated (QCCC, 2016)

Whistleblowing to Expose Health Care Fraud

Health care fraud is a type of white-collar crime that involves the filing of dishonest health care claims in order to turn a profit. Fraudulent health care schemes come in many forms. Practitioner schemes include: individuals obtaining subsidized or fully-covered prescription pills that are actually unneeded and then selling them on the black market for a profit; billing by practitioners for care that they never rendered; filing duplicate claims for the same service rendered; altering the dates, description of services, or identities of members or providers; billing for a non-covered service as a covered service; modifying medical records; intentional incorrect reporting of diagnoses or procedures to maximize payment; use of unlicensed staff; accepting or giving kickbacks for member referrals; waiving member co-pays; and prescribing additional or unnecessary treatment. Members can commit health care fraud by providing false information when applying for programs or services, forging or selling prescription drugs, using transportation benefits for non-medical related purposes, and loaning or using another's insurance card (Legal Information Institute, 2018).

When a health care fraud is perpetrated, the health care provider passes the costs along to its customers. Because of the pervasiveness of health care fraud, statistics now show that 10 cents of every dollar spent on health care goes toward paying for fraudulent health care claims. The World Health Report (2010_ estimated that about 20-40% of all health sector resources are wasted and highlighted health care leakages-waste, corruption and fraud-as the ninth leading source of inefficiency of health systems.

In the United States, according to the Federal Bureau of Investigation, healthcare fraud costs taxpayers over \$80 billion annually. From January 2009 through September 2013, the US federal government recovered \$17 billion in false claims alone. Federal and state laws that may involve whistleblowing include: False Claims Act (Qui Tam), 31 U.S.C. § 3730(h) – fraudulent billing by Medicare healthcare providers (hospitals, nursing homes, physician practices, etc.), drug and medical device manufacturers and suppliers; Georgia False Medicaid Claims Act, O.C.G.A. § 49-6-168 et seq. – fraudulent Medicaid claims submitted to the state Medicaid program; Fair Labor Standards Act, 29 U.S.C. § 218C (enacted Sec. 1558 of the ACA) – whistleblower protection for insurance company employees and others reporting violations of insurance reforms under Title I of ACA (e.g., prohibited coverage denials); False Claims Act (Qui Tam), 31 U.S.C. § 3729 – fraudulent bills or payments involving federal funds sent or made through a healthcare exchange established under the ACA; Stark Law/Anti-Kickback Statute, 42 U.S.C. § 1395nn (Stark), 42 U.S.C. § 1320a-7b(b) (AKS) – illegal referral fees or kickback arrangements between hospitals, surgery centers and healthcare facilities and physicians or other persons or entities for treating and referring patients for treatment; Sarbanes Oxley Act, 18 U.S.C. § 1514A – financial or other misrepresentations and fraud by public healthcare companies (for example, hospital operators); Occupational Safety and Health Act (OSHA), 29 U.S.C. § 660(c) – protection for employees and others reporting serious safety violations at healthcare facilities affecting patients or employees (violence against patients, inadequate care, unsafe conditions, etc.).

In an extreme case, a Detroit based oncology physician, Dr. Farid Fata, gave unnecessary treatments to 553 patients at a Detroit-area cancer center (Michigan, USA) in order to benefit from substantial health insurance claims totaling at least 17 million dollars. He was unmasked as a fraud by George Karadsheh, who took a job in 2011 as an office manager for Dr. Fata's rapidly expanding oncology practice in suburban Detroit. He was informed by another oncologist working in the practice and two nurse practitioners that patients were given chemotherapy and other treatments by Dr. Fata when they didn't have cancer. Karadsheh contacted an attorney – David Haron - he knew who handled whistleblower cases. Haron wasted no time and called the Department of Justice. George Karadsheh was willing to put everything on the line. "My job was at stake. My livelihood," he explained. "Even my own personal safety. "I wasn't looking at the patients anymore as being treated," Karadsheh said. "I looked at it as a burning building with people inside. ...I had to make it stop and I had to make it stop quickly. When he filed a lawsuit under the False Claims Act on Aug. 5, 2013, the so-called qui tam civil lawsuit joining Karadsheh and the government as co-plaintiffs — he triggered a legal process. Dr. Fata was convicted and sentenced to 45 years in prison for health care fraud. Dr. Fata pleaded guilty to sixteen counts—thirteen counts of health-care fraud, one count of conspiracy to pay and receive kickbacks, and two counts of promotional money laundering. He is currently appealing his sentence (US Sixth Circuit, 2016). George Karadsheh had been a federal whistle-blower before, and was very familiar with the legal processes involved. Government whistle-blower laws, including the False Claims Act used in this case, create a path for private citizens to help the government. The law requires secrecy for two reasons: to protect the government's investigation, and to protect the whistle-blower from retaliation and from contest to a financial stake in the outcome. In the Fata case, where the convicted doctor has surrendered more than \$10 million to the government, Karadsheh's share of 15-30 percent is at least \$1.5 million. The financial reward is rarely the sole motivation. The reward is taxable; lawyers typically get 20 to 30 percent; and whistle-blowers typically lose their jobs.

FUTURE RESEARCH DIRECTIONS

The internet, and associated utilization of health information systems management has been a major asset in improving medical documentation, simplifying payments and financial management, enhancing the scope of medical research using data linkage techniques, developing digital health technologies as well as internet monitored medical devices – Internet of Things. Largely unanticipated risks related to these benefits include: cybersecurity threats which may lead to theft of sensitive patient data and their sale on the dark web; financial internet fraud which may lead to diversion of large amounts of health care organizations' money into private accounts by criminally minded staff and external associates; medical research fraud, which is somewhat made easier by the use of internet resources to falsify data; and cyberattacks on internet controlled medical devices (Trend Micro, 2017). Contemporary health sector whistleblower activities are also strongly related to the use of the Internet, especially social media and online media outlets. Understanding factors that motivate whistleblowers in the health sector to utilize social or online media channels to publicize their concerns globally is an area worthy of research.

Future research directions should aim to adequately understand the scope and depth of vulnerabilities faced by health care sector in relation to whistleblowing and the use of internet or dark web, and to introduce appropriate ethics training, internal policies, cybersecurity upgrades, and appropriate comprehensive

and adaptive legislation which address the nexus between whistleblowing and the internet, in order to reduce its risks and maximize its benefits. For example, laws on external whistleblowing may require reporting first to institutional anti-corruption, regulatory boards and not to internet-based media, given the irreparable damage that such reports may cause to organizations if the whistleblower's claims turn out to be inaccurate, or if the reporting is motivated by vengeance or other ignoble aims.

In the area of financial fraud, web-based approaches for preventing financial fraud in healthcare settings, such as data mining based on Knowledge Discovery from Databases (Joudaki, Rashidian, Minaei-Bidgoli et al, 2015) should be explored for adaptation and general application. Internal controls in the form of policies and procedures are also important for controlling financial fraud in the health sector, most of which are currently carried out through illegal online funds transfers. For example, Hohepa Morehu-Barlow, a finance officer with Queensland Health, Australia, defrauded his employee to the tune of \$16.69 million in 65 fraudulent transactions between October 2007 and December 2011. A single fraudulent online transaction of \$11 million of public funds paid to Healthy Initiatives and Choices (HIC), a trading name registered to Hohepa in November 2011 raised audit queries which eventually led to his conviction (Crime and Misconduct Commission Queensland, 2013). Research geared towards the development of best practice standards internal audit controls is essential to prevent health care financial fraud.

Fraud related to research misconduct in healthcare requires renewed and expanded oversight powers devolved to Institutional Health Ethics Boards. An example of such expanded oversight powers relates to the ability to monitor research that is already approved in order to deter, detect and reduce health research fraud (Pickworth, 2000). Online tools such as protocols to detect fraud in web-based online research are particularly pertinent (Ballard, Cardwell and Young, 2019).

CONCLUSION

Whistleblowing may count as a crime or a virtue depending on the setting. Paramount in whistleblowing activities is the need to ensure that a violation has indeed been committed before reporting internally or externally. Healthcare workers have a responsibility to raise concerns about patient safety and unethical or illegal conduct. Yet, as shown by several of the case studies discussed in this chapter, those who raise serious concerns are often treated badly by senior colleagues, their employing organisations and the bodies that should protect whistleblowers. This paradox is because whistleblowers raise concerns that, if made public, would embarrass the organisation or senior and powerful individuals, who are considered less dispensable than the whistleblower. This chapter shows that whistleblowing is a vital instrument in uncovering criminal activity in the health sector, and may be superior to traditional approaches such as the longstanding use of peer review in excluding fraud in research work.

In nations where expressly stated legal whistleblower protections exist, and where external whistleblowers who correctly report criminal conduct are duly compensated financially, external whistleblowing may be worth the risks. Generally, internal whistleblowing represents the ideal approach to raising concerns about criminal activity. For internal mechanisms to be credible, high standards of organizational ethics and governance are indispensable. Criminal activity in the health sector is rare but carries significant risks for patient safety and financial sustainability of healthcare organizations. Internal and, rarely, external whistleblowing may facilitate risk management efforts for this significant leakage of health care resources.

REFERENCES

- Awofeso, N. (2017). Improving efficiency and reducing fraud in UAE's health insurance market. *Journal of Financial Markets*, 1(1), 7–16. Retrieved from <http://www.alliedacademies.org/articles/improving-efficiency-and-reducing-fraud-in-uaes-health-insurance-market.pdf>
- Ballard, A. M., Cardwell, T., & Young, A. M. (2019). Fraud detection protocol for web-based research among men who have sex with men: Development and descriptive evaluation. *JMIR Public Health and Surveillance*, 5(1), e12344. doi:10.2196/12344 PMID:30714944
- Bolsin, S., Pal, R., Wilmshurst, P., & Pena, M. (2011). Whistleblowing and patient safety: The patient's or the profession's interests at stake? *Journal of the Royal Society of Medicine*, 104(7), 278–282. doi:10.1258/jrsm.2011.110034 PMID:21725092
- Bundaberg Hospital Commission of Inquiry Report. (2005). Retrieved from <https://www.casewatch.net/foreign/patel/interimreport.pdf>
- Canadian Nurses Association. (1999). *I see and I'm silent; I see and I speak out – the ethical dilemma of whistleblowing*. Retrieved from https://www.cna-aic.ca/~media/cna/page-content/pdf-en/ethics_pract_see_silent_november_1999_e.pdf
- Clancy, C. M., Farquhar, M. B., & Sharp, B. A. (2005). Patient safety in nursing practice. *Journal of Nursing Care Quality*, 20(3), 193–197. doi:10.1097/00001786-200507000-00001 PMID:15965381
- Crime and Misconduct Commission Queensland. (2013). *Fraud, financial management and accountability in the Queensland public sector - an examination of how a \$16.69 million fraud was committed on Queensland Health*. Author.
- Dyer, O. (2005). Consultants who misled Shipman inquiry are found guilty of misconduct. *BMJ : British Medical Journal*, 331(7524), 1042. doi:10.1136/bmj.331.7524.1042-d PMID:16269475
- Fletcher, J. J., Sorrell, J. M., & Silvia, M. C. (1998). Whistleblowing as a failure of organizational ethics. *Online Journal of Issues in Nursing*, 3. Retrieved from <http://ojin.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Vol31998/No3Dec1998/Whistleblowing.aspx>
- Forster, P. (2005). *Queensland health system review – final report*. Brisbane: Queensland Parliament. Retrieved from <https://www.parliament.qld.gov.au/documents/tableOffice/TabledPapers/2005/5105T4447.pdf>
- Gee, J., & Button, M. (2015). *The financial cost of healthcare fraud 2015 – what data from around the world shows*. London: PKK Littlejohn LLP. Retrieved from <http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/The-Financial-Cost-of-Healthcare-Fraud-Report-2015.pdf>
- Guthrie, C. P., & Taylor, E. Z. (2017). Whistleblowing on Fraud for Pay: Can I Trust You? *Journal of Forensic Accounting Research*, 2(1), 1–19. doi:10.2308/jfar-51723
- HCCC. (2003). *Investigation report – Campbelltown and Camden hospitals, Macarthur Health Service*. Sydney: Health Care Complaints Commission. Retrieved from <https://trove.nla.gov.au/work/9673576?selectedversion=NBD25282706>

Heintzelman, C. (2003). The Tuskegee Syphilis Study and Its Implications for the 21st Century. *The New Social Worker*, 10, 4. Retrieved from http://www.socialworker.com/feature-articles/ethics-articles/The_Tuskegee_Syphilis_Study_and_Its_Implications_for_the_21st_Century/

Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., & Arab, M. (2014). Using data mining to detect health care fraud and abuse: A review of literature. *Global Journal of Health Science*, 7(1), 194–202. doi:10.5539/gjhs.v7n1p194 PMID:25560347

Keenan, J. P. (2000). Blowing the whistle on less serious forms of fraud: A study of executives and managers. *Employee Responsibilities and Rights Journal*, 12(4), 199–217. doi:10.1023/A:1013015926299

Legal Information Institute. (2018). *Health Care Fraud: An Overview*. Retrieved from https://www.law.cornell.edu/wex/healthcare_fraud#

McDonald, S., & Ahern, K. (2002). Physical and Emotional Effects of Whistle blowing. *Journal of Psychosocial Nursing and Mental Health Services*, 40(1), 14–27. doi:10.3928/0279-3695-20020101-09 PMID:11813350

MacDougall, R. D. (2015). Whistleblowing: Don't Encourage It, Prevent It Comment on "Cultures of Silence and Cultures of Voice: The Role of Whistleblowing in Healthcare Organisations". *International Journal of Health Policy and Management*, 5(3), 189–191. doi:10.15171/ijhpm.2015.190 PMID:26927590

Nair, S. K. (n.d.). The ethicality of whistleblowing and its implications for human resource management. *Indian Journal of Industrial Relations*, 38, 96–112.

National Health and Medical Research Council. (2018). *National Statement on Ethical Conduct in Human Research*. Canberra: NHMRC. Retrieved from <https://nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018#block-views-block-file-attachments-content-block-1>

Ogungbure, A., A. (2011). The Tuskegee Syphilis Study: Some Ethical Reflections. *Thought and Practice: A Journal of the Philosophical Association of Kenya*, 3, 75-92.

Pellegrino, E. D. (1995). Toward a virtue based normative ethics for the health professions. *Kennedy Institute of Ethics Journal*, 5(3), 253–274. doi:10.1353/ken.0.0044 PMID:10144959

Piper, D. L. A. (2015). *Whistleblowing – an employer's guide to local compliance*. London: DLA Piper. Retrieved from <https://www.dlapiper.com/en/us/insights/publications/2015/06/whistleblowing-law-2015>

Queensland Crime and Corruption Commission. (2017). *Australia's first criminal prosecution for research fraud - A case study from The University of Queensland*. Brisbane: The State of Queensland Crime and Corruption Commission.

Ramanathan, T. (2014). Law as a tool to promote healthcare safety. *Clinical Governance*, 19(2), 172–180. doi:10.1108/CGIJ-03-2014-0015 PMID:26855615

Ray, S. L. W., & Ethics, O. (2006). Whistleblowing and Organizational Ethics. *Nursing Ethics*, 13(4), 438–445. doi:10.1191/0969733006ne882oa PMID:16838574

Rickman, A. (2017). How China and the US are emboldening whistle-blowers in the fight against corporate corruption. *South China Morning Post*. Retrieved from <https://www.scmp.com/comment/insight-opinion/article/2121681/how-china-and-us-are-emboldening-whistle-blowers-fight>

Rossiter, E. J. (n.d.). Reflections of a whistle-blower. *Nature*, 11(357), 434 - 6.

Stericycle Expert Solutions. (2019). *Recall index, Q4, 2018*. Retrieved from <https://www.stericycleexpertsolutions.com/wp-content/uploads/2019/02/ExpertSolutions-RecallIndex-Q42018-web.pdf>

Stroebe, W., Postmes, T., & Spears, R. (2012). Perspectives on Psychological Science. *Scientific Misconduct and the Myth of Self-Correction in Science*, 7, 670–688. doi:10.1177/1745691612460687

Thomas, S. B. (2000). *The Legacy of Tuskegee. The Body: The Complete HIV/AIDS Resource*. Retrieved from <http://www.thebody.com/content/art30946.html>

Trend Micro. (2017). *Cybercrime and Other Threats Faced by the Healthcare Industry – a TrendLabs Research Paper*. Retrieved from <https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf> Accessed 25 March 2019.

US Sixth Circuit. (2016). *USA Vs Farid Fata. File Name: 16a0283n.06*. Retrieved from <https://www.gpo.gov/fdsys/pkg/USCOURTS-ca6-15-01935/pdf/USCOURTS-ca6-15-01935-0.pdf>

Van de Verden, P. G., Pecoraro, M., Houwerzijl, M. S., & van der Meulen, E. (2018). (in press). Mental health problems among whistleblowers: A comparative study. *Psychological Reports*. doi:10.1177/0033294118757681 PMID:29451073

Webb, G. (2018). *Whistle-blowers and research fraud – we should reward not shoot the messenger*. Retrieved from <https://drgeoffnutrition.wordpress.com/2018/07/15/whistleblowers-and-research-fraud-dont-shoot-the-messenger/>

Wilmot, S. (2000). Nurses and whistleblowing: The ethical issues. *Journal of Advanced Nursing*, 32(5), 1051–1057.

Winker, M. A., Flanagan, A., Chi-Lum, B., White, J., Andrews, K., Kennett, R. L., ... Musacchio, R. A. (2000). Guidelines for Medical and Health Information Sites on the Internet: Principles Governing AMA Web Sites. *Journal of the American Medical Association*, 283(12), 1600–1606. doi:10.1001/jama.283.12.1600 PMID:10735398

World Health Organization. (2010). *World Health Report, 2010: Health Systems Financing – the path to universal coverage*. Geneva: WHO. Retrieved from https://www.who.int/whr/2010/10_summary_en.pdf

Wright, T. (2010). The Stoke CNEP Saga - how it damaged all involved. *Journal of the Royal Society of Medicine*, 103(7), 277–282. doi:10.1258/jrsm.2010.10k012 PMID:20406828

ADDITIONAL READING

Bolsin, S., Faunce, T., & Oakley, J. (2005). Practical virtue ethics: Healthcare whistleblowing and portable digital technology. *Journal of Medical Ethics*, 31(10), 612–618. doi:10.1136/jme.2004.010603 PMID:16199607

Faunce, T. (2004). Developing and teaching the virtue-ethics foundations of healthcare whistle blowing. *Monash Bioethics Review*, 23(4), 41–55. doi:10.1007/BF03351419 PMID:15688511

Callahan, E. S., & Dworkin, T. M. (1994). Who blows the whistle to the media, and why: Organizational characteristics of media whistleblowers. *American Business Law Journal*, 32(2), 151–184. doi:10.1111/j.1744-1714.1994.tb00933.x

Terry Morehead Dworkin, T. (1998). Internal vs. External Whistleblowers: A Comparison of Whistleblowing Processes. *Journal of Business Ethics*, 17(12), 1281–1298. doi:10.1023/A:1005916210589

KEY TERMS AND DEFINITIONS

Criminal Negligence: Reckless disregard for the lives or safety of other persons. In health care contexts, healthcare providers have a fiduciary responsibility for providing appropriate treatment to patients under their care. Many nations have laws that make overt negligence in the provision of healthcare a criminal offence.

Health Research Fraud: Intentional misrepresentation of the methods, procedures, or results of healthcare research. Behavior characterized as scientific fraud includes fabrication, falsification, or plagiarism in proposing, performing, or reviewing scientific research, or in reporting research results. Health research fraud is unethical and often illegal. A good example of such fraud with major ramifications is the measles-autism link published in the lancet but retracted in 2010 when it was confirmed that the study was conducted dishonestly and irresponsibly, using bogus data. Nevertheless, this erroneous link is partly responsible for increasing refusals of Measles containing vaccines by parents.

Healthcare Fraud: An intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party Healthcare fraud refers to illegal acts of misrepresentation and false claims in order to receive undue financial or healthcare advantages. Health care fraud accounts for between 2 and 10% of wasted health resources globally. The World Health Organization cites healthcare-related fraud as one of 10 leading causes of inefficiency in health systems. Web-based healthcare fraud is a major challenge, especially when signatories to health organizations' accounts siphon money into private bank accounts. Regular audits and electronic monitoring systems such as e-claims management services help to monitor and prevent healthcare fraud.

Patient Safety: Initiatives to assure freedom from accidental or preventable injuries produced by medical care. Emphasis is placed on the system of care delivery that prevents errors, learns from the errors that do occur, and is built on a culture of safety that involves health care professionals, organizations, and patients. With the expansion of internet technology in the use of medical devices such as cardiac pacemakers, patient safety is increasingly vulnerable to web-based attacks, which have serious repercussions.

Raising Concerns Policy: Otherwise labelled “freedom to speak up” and “internal whistleblowing” such policies provide standardization of internal channels for speaking up about illegal or unethical practices and provide support and required anonymity for the employee who raises a concern.

Relational Ethics: A contemporary approach to ethics that situates ethical action explicitly in relationship. An important context of such relationships is within organizations, in which employees and employers have roles and responsibilities. Organizational policies and codes of conduct (and in some nations, anti-defamation laws) usually explicitly prohibit employees from discussing or exposing company secrets to the media or third parties without management approval. Thus, external whistleblowers are implicitly violating the relational ethics of such organizations.

Veracity: Conformity to facts; accuracy. Veracity is often difficult to establish in whistleblowing contexts since most whistleblowers have only limited information on a specified issue. Consequently, a significant proportion of external whistleblowing incidents have been found to be false. Contemporary whistleblowing laws such as the 2019 law in Australia require whistleblowers to provide objective evidence as condition to raising concerns internally or externally.

Virtue Ethics: Person rather than action based ethical conduct. It analysis at the virtue or moral character of the person carrying out an action, rather than at ethical duties and rules, or the consequences of particular actions. When morally orthodox and benevolent, virtue ethics is closely aligned to the ethical principle of deontology – fulfilling a virtuous moral duty. Many whistleblowers claim that their decision to expose alleged wrongdoing in their organizations were motivated by the desire to act according to their moral character to prevent harm to innocent others.

Whistleblowing: Non-obligatory act of disclosing information about unethical or criminal activity in an organization. Internal (intra-organizational) whistleblowing is less damaging to organizational credibility and the careers of whistleblower than external whistleblowing – reporting to the media or anti-corruption or institutional ethics boards. The term whistleblower comes from the whistle a referee uses to indicate an illegal or foul play. Ralph Nader coined the phrase in the early 1970s to reduce stigmatization of individuals who report illegal activity, any of whom were at the time referred to as “rats” and “snitches”. There are no public cases of cybersecurity whistleblowers on record to date, but in countries like the United States where large organizations have minimum mandatory cybersecurity requirements and payments of up to 30% may be received for whistleblowing acts which lead to recovery of assets from the Securities and Exchange Commission, a strong potential exists for such cases to emerge.

Online Activism to Cybercrime

Anita W. McMurtry

Atlanta Metropolitan State College, USA

Larry D. Stewart

Atlanta Metropolitan State College, USA

Curtis L. Todd

Atlanta Metropolitan State College, USA

INTRODUCTION

Hactivism is a socially or politically motivated act of misuse of computer systems, the internet, or a technology hack; which can be traced three decades back to 1989, when DOE, HEPNET and SPAN (NASA) connected VMS machines worldwide and were penetrated by the anti-nuclear WANK worm (Moore, Shannon, & Brown, 2002). Subsequently, it appeared on criminal justice systems' radar from law enforcement, to the courts, and then to corrections. There is a new imperative to not only gain a better understanding of the intricacies of this problematic behavior when it rises to criminal activity, but also how best to safeguard society in general, as well as national and international public and private businesses, organizations and governmental agencies. This entry moves beyond mere definitions of how what was once considered another form of legitimate protest and activism by delving deeply into the psychology and practical ramifications of its emergence, which has quickly morphed into problematic cyber behavior and criminal activity perpetrated through the improper use of technological tools and digital platforms.

To construct a solid operational understanding of Hactivism, this entry first extends its context as a cybercrime to include a global perspective, as well as hacker cultural and ethical mindsets. Second, inherent dangers, as it relates to critical areas such as political elections, industry and corporations, international affairs, personal data, and national security, are explored to further contextualize Hactivism's evolution and real-world challenges in identifying, investigating and prosecuting criminals. Also, legal issues and implications for criminal justice systems are explored to firmly anchor the urgency in moving this virtual issue to the center of priorities. Finally, informed suggestions, recommendations and future research directions are provided.

HACKTIVISM: A CONTEXTUAL DEFINITION

Derived from combining the words "hack" and "activism", the term "Hactivism" was first coined in 1996 by Omega, a member of the hacker collective Cult of the Dead Cow (Dyer, 2018). The group created an organization espousing that freedom of information was a basic human right. The group designed software to circumvent censorship controls on the Internet that some governments used to prevent citizens from seeing certain content. Hactivism is mainly portrayed in society as the transposition of demonstrations, civil disobedience, and low-level information warfare into cyberspace (Dyer, 2018). Hactivists

DOI: 10.4018/978-1-5225-9715-5.ch022

are the modern equivalent of political protesters, and the rise in hacktivist activity may be due in part to the growing importance of the Internet as a means of communication. Besides hackers who are in it for profit, there are hackers who break into systems to point out security flaws, and there are those who want to bring attention to a cause. The latter however, typically come in the form of virtual political activists who have adapted their methods of dissent into digital platforms, an act known as Hacktivism. Individuals proclaiming themselves as “hacktivists” often work secretly, sometimes operating in discreet groups while other times operating as individuals with cyber-world identities all consistent with the stated purpose of gaining public access and power in today’s society (Sengupta, 2012).

BACKGROUND

Hacking originated in the 1960s via the Tech Model Railroad Club at Massachusetts Institute of Technology (Leeson & Coyne, 2005). These computer scientists were charged with “hacking” switch control systems of model trains, increasing their speed, making them more efficient. At this time, Artificial Intelligence was also introduced and brought about the first large mainframe computer system. Hacking became the solution in solving issues of the mainframe computer providing shortcuts and allowing the system to run quicker and simpler. Hacking in its infancy had little to do with malicious intent. The original goal was to advance computer usage and not impair it. Hacking then became a means of personal gain in the 1970s using phone systems. This activity was known as Phreaking, which is the act of carrying out illegal activity via the telephone system (Pavlik, 2017). Hacker gangs developed in the 1980s with the Milwaukee area’s 414 gang. These noted individuals were able to access unauthorized outside computer systems and cause serious damage and disorder. The 414 gang is one of the first to be detained legally for their cyber-crimes (Leeson & Coyne, 2005). Consequently, in 1984, the government made it illegal to gain unofficial entry into a computer system.

Hacking is prevalent not only on computer systems, but the Internet as well. Cornell University was impacted by an Internet worm named Morris in 1988. The offender was sentenced to three years of probation (Leeson & Coyne, 2005). In the 1990s the pressing need to control the massive growth of the hacker occupation birthed the Federal Government to plan a series of raids in 14 cities known as “Operation Sundevil.” The notion that the majority of hacking involves pranks by pubescent boys or inconsequential crime is outdated. Organized crime hackers seek more lucrative initiatives. Russian hackers also stole \$10 million from Citibank, and the Federal Government responded in 1998 through the creation of the National Information Infrastructure Protection Center. Hacking overall is a worldwide phenomenon and is projected to become worse overtime. Denial-of-Service (DDoS) attacks that shutdown systems of enterprises such as Yahoo!, eBay, and Amazon, cost the global economy billions in lost revenue. Hacking comprises of breaching passwords, generating e-mail bombs, DDoS intrusions, scripting and circulating viruses, worms, and Trojans, screening prohibited intellectually property, URL redirection, and web defacement (Leeson & Coyne, 2005).

Cyberattacks have gained national and international attention. In 2008, a group named Anonymous opened a number of cyberattacks to assist a range of political and social issues. The focus and purpose of the group spans from commercial to government to religious organizations. On January 7th, 2013, Anonymous issued a “We the People” request asking the White House (United States of America) to acknowledge dispersed denial-of-service (DDoS) incidents as an endorsed form of demonstration safeguarded by the First Amendment of the United States Constitution (Li, 2013). Alongside Anonymous’ position, commentators posit that Hacktivism expands to digital civil disobedience, even if success is

gained by means of disturbance of circulation of data. Current trends in cyberattacks are questionable to warrant First Amendment consideration. Research also implies that Hacktivism may develop over time to fall within the scope of First Amendment defense. An absolute ban on all methods of Hacktivism may take up socially prolific practices of cyberattacks as a manner of protest (Li, 2013).

In the age of global capital, a concise focus from the criminal justice system is paramount. A complete global interest on the issue of cybersecurity has yet to be developed to effectively protect the cyber realm. Trans-national law enforcement practices in 'cyberspace' are necessary in maintaining cybersecurity. New networks are needed and the relationship between the government and other agencies will need to span across our national borders. Improvements are underway amongst nations to cultivate the strength of the international police in order to respond to cybercrime and education regarding the ground level security measures (Broadhurst, 2006). As a result, scholars and practitioners with a vested interest in alleviating the issue of malicious attacks are encouraged to 'think globally - act locally.' The Council of Europe's Cybercrime and the United Nations against Transnational Organized Crime are consistently vying for a worldwide standard of civil protections. Critical infrastructure and critical information infrastructures must be protected globally to protect the government and other systems from various security breaches. Thus, hacktivist may view the lack of attention and care as fertile ground for planting and cultivating a message or ideology (Broadhurst, 2006).

HACKING IN THE 21ST CENTURY

Hacking practices in the 21st century consists of modifying computer hardware and digital devices. Hacking in today's culture also requires new and more powerful resources as well as education via forums as Web 2.0 services. The I-phone and I-pad are significant suppliers in the spread of hacking culture amongst consumers. In answering the newly set boundaries, the I-phone operative scheme was "hacked" with the intention of permitting consumers to connect functions not authorized by the original owner. The message of this I-phone adjustment can also be coined as "jailbreaking," emphasizing the restriction of Apple's software and the permissive tone of alteration (Magaudha, 2010). Kirsch (2014) also notes the 2013 Target breach immensely disturbing one third of the United States. According to the FBI, similar attacks will increase even in the midst of efforts, fueling the platform of using cyberspace for nation state and non-nation state purposes.

POTENTIAL DANGERS TO DEMOCRACY

Hacktivism generally operate under a non-political umbrella and express self or group defined ideas without them being analyzed by the society at large. Their anonymous identities give them a sense of declared power to represent or defend matters of concern that they feel are important to them and their communities. Lately, however, the Hacktivism term has been applied to protests against multinational organizations, governments, and even rural law enforcement agencies, and the tactics now include denial-of-service attacks on sites, as well as leaks of confidential documents to the public. Although hacktivists typically go after non-retail organizations, the fallout from these attacks can still affect millions of people. In order to carry out their operations, they have the capacity to create new technology or integrate or use a variety of software tools that are readily available on the Internet. Hacktivism may be used as a substitute for or complement to traditional forms of activism such as sit-ins and protest marches. This

has happened with the Occupy Wall Street and Church of Scientology protests, which involved both the physical presence of supporters in the streets and online attacks (Aviles, 2015). Hactivist attacks, in and of themselves, are not violent and do not put protestors at risk of physical harm – unlike participating in a street protest – but in some cases, Hactivism might incite violence. It also makes it possible to support geographically distant causes without having to travel there and makes it possible for geographically dispersed people with common goals to unite and act in support of a shared goal. Hactivists represent many categories and classes of hacking for the sake of activism. It disturbs certain segments of society when it becomes a source involved in illegally accessing someone’s digital information for a political or social cause (Lindgren, 2011).

POLITICAL ELECTIONS

Hactivists have gone after everyone from foreign governments and corporations to drug dealers and pedophiles. Police departments, hospitals, small towns, big cities and states also have come under attack. Online activists have successfully frozen government servers, defaced websites, and hacked into data or email and released it online. The general category for this type of hacker would be a “Grey Hat” Hacker. One class of hactivist activities includes increasing the availability of others to take politically motivated action online to influence desired outcomes involving actors of broad nation states, oligarchs, or private organizations. Political activism is nothing new, but taking it online through covert tactics is a major change. It does not matter whether one views hactivists as dangerous enemies of the state or as digital ‘Robin Hoods,’ stealing information from the powerful and distributing it to the masses, the truth is that Hactivism can sway public opinion (Lindgren, 2011). However, a hactivist must find vulnerabilities within a system before covert political actions can take place.

American political elections are often the targets of threats by Russian, Chinese, and Iranian hactivists. Political elections are public and overseen by individual states and administered by local municipalities. Many of the voter systems are out of date and plagued with a variety of weaknesses. Efforts on behalf of the federal government to harden these voting systems have, in some cases, been met with suspicion by local and state officials wary of losing their autonomy. The U. S. Department of Homeland Security (DHS), the federal agency in charge of election security, indicates that they can help states or municipalities only if they request assistance; however, its recommendations, like those of other federal agencies, are not mandatory. But local election officials often lack the expertise needed to evaluate their systems’ liabilities and in addition, they have been known to be careless about securing those systems: software updates go uninstalled; machines are left unguarded and unlocked; and election programming and vote tabulation are often outsourced to third-party vendors that may have their own exposures (Leithauser, 2012). Americans, feeling victimized by election hacking, are more aggressive than ever in voicing concern and questioning over what is being done beyond government actions to prevent elections hacking. While the response describing the implementation of the DHS Cybersecurity agency was cited the most, other actions are receiving notoriety: social media firms are aggressively tampering down the use of their entities in campaigns; states with extremely large populations are attempting to pass election security policies; and both public and private firms are committing themselves to using smart technology to monitor foreign actors. An increase in new Hactivism is now the top anti-establishment online tool for achieving a diverse set of causes around the globe. Hactivists are deploying a range of tactics from temporarily shutting down servers to disclosing personal records and corporate information (Klein, 2015).

PERSONAL RECORDS

A group of nearly 3000 hacktivists under the name “Operation Payback” are on record as launching online attacks against PayPal, MasterCard, and Visa, briefly knocking the three financial services’ sites offline and attempting to prevent consumers from accessing their online banking and financial services. The hacktivists retaliated against the three companies for severing ties with WikiLeaks, an online repository for whistleblower data that had recently included thousands of secret communications from the U.S. State Department and other world governmental agencies (Anonymous, 2016). The key components of this operations involved records consisting of financial statements, income statement, balance sheet, and statement of cash flows. As a whole, these financial statements are designed to present a complete picture of the financial condition and results of a person or a business. A case can be made for each of the financial statements being the most important, though the ultimate answer depends on the needs of the user or their value to another interested party. The key points favoring each of these financial statements as being the most important to a hacktivist are income statements, balance sheets, and statement of cash flow.

The most important financial statement for the hacktivist is likely to be the income statement, since it reveals the ability of a business to generate a profit. Also, the information listed on the income statement is mostly in relatively current dollars, and so represents a reasonable degree of accuracy. The balance sheet is likely to be ranked lower by hacktivist, since it does not reveal the results of operations and some of the numbers listed in it may be based on historical costs, which renders the report less informative. The balance sheet is of considerable importance when paired with the income statement, since it reveals the amount of investment needed to support the sales and profits shown on the income statement. The best candidate for most important financial statement to the hacktivist is the statement of cash flows, because it focuses solely on changes in cash inflows and outflows (Schwartz, 2012). This report presents a more clear view of an individual or company’s cash flows than the income statement, which can sometimes present skewed results, especially when accruals are mandated under the accrual basis of accounting. The two statements that provide the most information to the hacktivist are the income statement and balance sheet, since the statement of cash flows can be constructed from these two documents. There are various ways hacktivists could exploit this type of information. The most common and easiest way is to simply print and write fraudulent checks in the name of the target, but unlike hackers for illegal gain, hacktivist usually operates on a higher level of morality that is aimed at highlighting injustices or frauds that are being perpetrated on the masses or those perceived as innocent victims (Schwartz, 2012).

TRADE SECRETS

Trade secrets theft or related exposures are often thought to be a ripe area for hacktivists activities. A trade secret is a formula, practice, process, design, instrument, pattern, commercial method, or compilation of information not generally known or reasonably ascertainable by others to the degree that a business can obtain an economic advantage over competitors or customers. Trade secrets can include advertising strategies, sales methods, and manufacturing processes. They also can be industry-specific, such as a company’s food or drink recipe. For example, the recipe for Coca-Cola is probably one of the most famous and well-kept trade secrets in the world today. The trade secrets theft industry – with consumers, suppliers, and information systems – is thriving on the data collected and stolen from electronic archives. There is a major market for stolen trade secrets and data relating to business advancements;

the technicians who do the hacking are not the ones who collect the data and do the collating and automating the fraud and subsequently collecting the profit. Threat actors come in many forms: malicious insiders, competitors, nation states, transnational organized figures and hacktivists (Dissecting a hacktivist attack, 2012). Hacktivists seek to expose sensitive corporate information, potentially including trade secrets, to advance political or social ends. These groups have used cyber intrusion skills and data gleaned from disgruntled insiders to obtain and publish Personally Identifiable Information (PII) and sensitive business information of key executives, employees, and business partners. Hacktivists have the technical knowledge and capabilities to steal trade secrets, and they could partner with other threat actors for ideological or financial reasons. Intentional theft of trade secrets can constitute a crime under both federal and state laws (Bradshaw, 2011).

The most significant law dealing with trade secret theft is the Economic Espionage Act of 1996, which made the theft, transmission, or receipt of trade secrets a federal crime. Many states have also enacted laws making trade secret infringement a crime. Corporate executives around the world regularly make decisions based on expectations about the future. Choices related to new product launches, expanding strategic business relationships, investment in capital projects, and research and development expenditures are each grounded, in part, on companies' expectations about the future. The challenge of trade secret theft is too large for any one government, company or organization to deal with alone. Only a collective focus on this issue will help improve innovators' ability to secure their most critical information and intellectual property (Bradshaw, 2011). Hacktivist might be involved in stealing or sharing trade secrets in an attempt to expose a company's unfair treatment of a class of individuals or some specific wrong doings.

ECONOMIC PROSPERITY

The economy is the process or system by which goods and services are produced, sold, and bought in a country or region. The U.S. economic environment is characterized by specializing in producing public goods and finances these goods with different revenue streams. Public goods benefit a large group of people and are collectively used by anyone. Goods can be owned exclusively and enjoyed individually, and can be bought and sold in market transactions; the ability to pay determines their allocation. The U.S. economic crisis resulted in social activism and provides ripeness for Hacktivism. The Occupy Wall Street Movement reflected social trends against economic inequality, which was intensified by the economic crisis. The main purpose of this social manifestation was to demand more political and socio-economic equality. They believed that larger corporations and global financial banks were misrepresenting the lower and middle class during the economic crisis. Further, it asserted that telecommunications and its associated technology not only contributes to economic weaknesses, but also affects intelligence operations (collection, analysis and dissemination) and promotes the complexity of war ramifications. Correspondingly, this lays a formidable foundation for hacktivist intervention (Aviles, 2015).

EFFORTS TO COMBAT HACKING

Law enforcement have made remarkable strides in contesting hacking throughout the country and globally. New systems connecting patrol and other organizations within government, systems connecting police and private organizations, and systems of patrol throughout the country's boundaries. Globally, two innovative treaty resources supply a complete foundation for the necessary cross-border patrol and

agent collaboration necessary in fighting cybercrime. The first resources, the Council of Europe's Cyber-Crime Convention, developed through resolution and aimed as an area contrivance with international credibility. The latter is the United Nations Convention against Transnational Organize Crime, which is universal in reach but circuitously manages Cybercrime when implemented by criminal associations in connection to serious crimes (Sangkyo & Kyungho, 2014).

In 2002 the Cybersecurity Enhancement Act provided a provision for privacy protection and a computer crime sentencing detail guide for enhanced penalties. In 2009 China brought forth an Amendment to the Criminal law of China (VII), which added "Hacker" to the Criminal code in order to be able to legally punish hacking. Shortly after in 2011, the Supreme People's Court held a trial to increase penalties for buying and selling materials for hacking purposes. After the trial, acts such as providing software would be punishable for up to ten years. Table 1 provides a comparison of each country's criminal law.

THE COMPUTER FRAUD AND ABUSE ACT

Computer crimes are primarily addressed by the Computer Fraud and Abuse Act of 1986 (CFAA). The CFAA makes it unlawful for any person to access a protected computer without authorization. It also forbids a person who has a legitimate and authorized right of access from exceeding the authorized access. If either type of access results in the person's obtaining information from the protected computer and the conduct involves interstate or foreign communication, then a violation of the Act is established. The CFAA also prohibits activities such as the dissemination of malicious software and trafficking in stolen passwords. The CFAA allows any person who suffers damage or loss by reason of a violation of the statute to maintain a civil action to obtain compensatory damages and injunctive relief or other equitable relief (Milone, 2013).

USA PATRIOT ACT

United States' President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) into law on October 26, 2001. This Act of Congress provides law enforcement with sweeping powers and raised concern among privacy advocates. In essence, the Act seeks to protect the national infrastructure

Table 1. Comparing each country's criminal law

	Korea	Germany	USA	China
Legislation	Network Act, 48	Criminal Law, 202(a)	CFAA (18 U.S.C 1030)	Criminal Law, 285
Criterion for punishment	Access abusing their authority	Access without authorization	Exceeds authorized access	Intrusion actions
Penalty (imprisonment)	3 years	3 years	Over 10 years	3-7 years
Feature	In distributed laws	In Criminal Law	Severe punishment	Punish acts of indirect

Sangkyo, O. Kyungho, L. (2014). The Need for Specific Penalties for Hacking in Criminal Law. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4083268/>

by easing the restrictions placed on electronic surveillance and facilitating the prosecution of cybercrime by amending many provisions in the CFAA. These amendments lower jurisdictional hurdles relating to protected computers and damages, and increase penalties for violations. Expanding the scope of “protected computers.” Before the amendments in section 814 of the Act, the CFAA defined “protected computer” as a computer used by the federal government or a financial institution, or one used in interstate or foreign commerce or communication. This definition did not explicitly include computers outside the United States. Because of the interdependency of global computer networks, system crackers from within the United States increasingly targeted systems located entirely outside of this country. In addition, computer criminals in foreign countries frequently routed communications through the United States as they gained access from systems located in one foreign country to another. In such cases, the lack of any U.S. victim discouraged U.S. law enforcement agencies from assisting in any foreign investigation or prosecution. Section 814 of the Act amends the definition of “protected computer” to clarify that this term includes computers outside of the United States, so long as they affect interstate or foreign commerce or communication of the United States. This allows the United States to use speedier domestic procedures to join in international computer crime investigations. In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States.

The CFAA previously had no special provision that would augment punishment for criminals who damage computers used in connection with the judicial system, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over \$5,000 loss or meet one of the CFAA’s other special requirements. These systems, however, serve critical functions and arguably justify felony prosecutions even where the damage is relatively slight. Amendments in section 814 of the USA PATRIOT Act also created a section to address this issue. Under this provision, a criminal violates federal law by damaging a computer “used by or for a government entity in furtherance of the administration of justice, national defense, or national security,” even if that damage does not result in provable loss over \$5,000. Under previous law, first-time offenders who violate section 1030(a)(5) could be punished by no more than five years’ imprisonment, while repeat offenders could receive up to ten years. It was argued, however, that this five-year maximum did not adequately take into account the seriousness of their crimes. In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4). Section 814 raises the maximum penalty for violations arising out of damage to protected computers to ten years for first offenders, and twenty years for repeat offenders. Congress also chose to eliminate all mandatory minimum guidelines sentencing for section 1030 violations. New legislation has also been introduced to further increase these penalties (Milone, 2013).

IMPLICATIONS FOR THE CRIMINAL JUSTICE SYSTEM

Law enforcement agencies and their processes play a pivotal role in criminal justice systems’ overall goal of controlling crimes and imposing penalties on those violating laws. Their important work is the catalyst for the involvement of subsequent system components. Central to the duties and responsibilities of law enforcement officers is taking reports and investigating crimes, as well as gathering evidence. They are also responsible for protecting evidence, conducting follow-up investigations and are frequently

called upon to give testimony in court proceedings (Concer, Paynich & Gingerich, 2013). At any point during the course of these duties, there are formidable challenges as it relates to Hacktivism. Though there has been some success in the arrest of individual hackers, usually high profile personalities, opportunities yet persist.

The courts also encounter problematic areas. Jurisdictions are often blurred lines that traverse local, state, national and international boundaries. Complications also occur because the world of Hacktivism is populated with thousands of bad actors and groups – often leaderless – amounting to a decentralized network of criminals masquerading as self-proclaimed activists (Denning, 2015). Since it is frequently difficult to identify specific hacking organizations, groups and individuals, criminal justice systems' response to the criminal actions of perpetrators from investigation, prosecution to sentencing, the urgency is all the more real. Time is always of importance, especially given the capriciousness of cyberspace and the lack of perpetrators needing a geographical locale. This significantly impedes efforts to shut them down.

Human and financial resources are key in launching, sustaining and insuring that persistent countermeasures are in place, starting with an effective cybersecurity workforce. Disturbingly, the current availability level of cybersecurity professionals is not meeting today's market demands (Perhach, 2018). When these systems fail, criminal justice networks will require an unprecedented amount of technological advantages at their disposal to adequately investigate and prosecute cybercriminals operating under the guise of hacktivists. Cooperation among federal and international jurisdictions is often warranted. This will occur when damages are significant, established cybercrime laws have been violated and there is a mutual agreement among countries.

CHALLENGES TO PREVENT HACKING

As challenging as hacktivist attacks are, they can be met if the United States and like-minded countries undertake the awesome tasks to do so. The first step would be to organize properly, working across national jurisdictions to ensure the stability of the global internet system. An international cyber strategy made up of capable nations consisting initially of the United States, and others could join together to create international standards, protect infrastructures and undertake common approaches to develop a more resilient future internet. Such an approach could both go far beyond what current institutions can do independently, but also build on and make enforceable standards and other actions undertaken by other entities. The key is combined efforts by like-minded stakeholders across international borders, rather than reliance on narrowly focused groups from one or a few countries – an approach which has been a miserable failure (Klein, 2015).

Hacktivism has become an integral part of modern life, and modern institutions are necessary to safeguard it. It has the obvious characteristic of simultaneous maneuvers across multiple nationwide boundaries, with the potential of creating universal impacts. An international cyber strategy would work best by focusing on three areas. First, it could protect the critical infrastructure backbone of the internet – those entities that are systemically important to internet stability. Second, it could establish an enforceable set of standards for the rapidly emerging so-called “internet of things,” which is now inclusive of a range of consumer household products. An example of this is the blue tooth technology used for cell phones. Third, the national members tasked with developing the strategy would have all been subject to Hacktivism, cyber espionage, politically motivated intrusions, and criminal activity. The strategy then could help coordinate international responses to these activities, including the sharing of data, analysis and tools, and undertaking coordinated campaigns and responses (Klein, 2015).

RECOMMENDATIONS

The following directional recommendations for scholars and practitioners are important steps in making sure that Hacktivism remains at the center of emerging criminal justice issues needing to be addressed through research. Further, it is an issue that must be incorporated across all landscapes, from the classroom and professional conferences to the more complex process of lawmaking. The study of Hacktivism has a future in political science and in social science more broadly. This indicates that researchers must fully conceptualize the range of issues that conforms to Hacktivism's peculiar characteristics, and make it a useful laboratory for addressing certain kinds of social scientific inquiries. Contemporary conclusions about Hacktivism are by necessity more speculative.

There are two countervailing forces that are interacting to shape Hacktivism's future: first, the post September 11, 2001 terrorist attacks against the United States (9/11) security environment, and second, the expanding domain of international political affairs. The events of the 9/11 changed the context for Hacktivism in two crucial ways. First, they increased U.S. vigilance towards all potential security threats, including cyberterrorism. Second, the immediate and longer-term political consequences of 9/11 have led to the deepening of various international conflicts implicated in international Hacktivism (Milone, 2002). Increased vigilance against the prospect of cyberterrorism has had its most tangible impact in the increased penalties for all forms of computer hacking – potentially including much of hacktivist activity. Though the USA PATRIOT Act amended the Computer Fraud and Abuse Act (CFAA) to lower jurisdictional hurdles relating to protected computers and damages, and increase penalties for violations (Milone, 2002), additional research should be conducted to ensure that legislative and regulatory mandates are available and consistent with both state and federal laws.

CONCLUSION

The lens in which to properly view Hacktivism must be all encompassing to include a global perspective of cybercrimes. Also, the full range of noted and potential threats against targeted political elections, industry and corporations, international affairs, personal data, and national security are rapidly increasing and evolving. Further, this rise in criminal behavior uniquely positions criminal justice systems to reinvent how they research, investigate, and hold offenders accountable. Systems are beyond the proverbial “crossroad” regarding Hacktivism; rather, they are in the middle of an important battle. Leadership must be from the front of this issue, not the back. It is within the capacity of well-balanced, financed, and resourced collaborations to do more. Effectively countering Hacktivism rests with eradicating two basic, yet flawed ideological assumptions. First, this is complex work – there is nothing simple or easy regarding the levels of human and technological resources needed to launch credible and sustained proactive, as well as reactive responses. Second, as previously noted, this is a network, therefore a formidable and equally robust response from local, state, regional, national and international network must be activated. The levels of cooperation among all stakeholders must be unprecedented. Equally, aggressive levels of human and technological resources must be ensured and not be prohibitive. From perhaps well-meaning protest activities perpetrated via the internet to obvious violations of laws, Hacktivism is the new intractable imperative for criminal justice systems.

REFERENCES

- Anonymous. (2016). Hacktivist groups can provide accountability. *USA Today*, 144(2853), 5-6.
- Aviles, G. (2015). *How U.S. political and socio-economic trends promotes hacktivist activity* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses.
- Bradshaw, T., & Cookson, R. (2011, February 7). Hacktivist group in switch to securities. *The Financial Times*, p. 15.
- Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408–433. doi:10.1108/13639510610684674
- Concer, J., Paynich, R., & Gingerich, T. (2013). *Law enforcement in the United States*. Burlington, MA: Jones & Bartlett Learning.
- Denning, D. (2015, September 8). The rise of hacktivism. *Georgetown Journal of International Affairs*. Retrieved from <https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism>
- Dissecting a Hacktivist Attack. (2012). *Computer Fraud & Security*, (6), 3.
- Dyer, T. (2018). *Hacktivist or cyberterrorist? Understanding the difference between hacktivism and cyber terrorism* (Doctoral dissertation). ProQuest Dissertations and Theses.
- Kirch, C. (2014). The Grey Hat Hacker. Reconciling Cyberspace Reality and the law. *N. Ky. L. Rev*, 41, 383.
- Klein, J. (2015). Deterring and dissuading cyberterrorism. *Journal of Strategic Security*, 8(4), 23–38. doi:10.5038/1944-0472.8.4.1460
- Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *Journal of Economics & Policy*, 1, 511.
- Leithauser, T. (2012). FBI targets ‘hacktivist’ groups, arrests alleged LulzSec members. Cybersecurity Policy Report.
- Li, X. (2013). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology*, 27, 301.
- Lindgren, S., & Lundström, R. (2011). Pirate culture and hacktivist mobilization: The cultural and social protocols of #wikiLeaks on twitter. *New Media & Society*, 13(6), 999–1018. doi:10.1177/1461444811414833
- Magaudda, P. (2010). Hacking Practices and their relevance for Consumer Studies: The example of the ‘jailbreaking’ of the iPhone. *Consumers, Commodities, and Consumption*, 12(1), 12–11.
- Milone, M. G. (2002). Hacktivism: Securing the national infrastructure. *Business Lawyer*, 58(1), 383–413.
- Milone, M. G. (2003). Hacktivism: Securing the national infrastructure. *Knowledge, Technology & Policy*, 16(1), 75–103. doi:10.1007/12130-003-1017-5
- Pavlik, K. (2017). Cybercrime, hacking, and legislation. *Journal of Cybersecurity*, 1(1).

Perhach, P. (2018, November 7). The mad dash to find a cybersecurity force. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html>

Schwartz, M. J. (2012, September 28). PNC bank hit by crowdsourced hacktivist attacks. *Information-week – Online*. Retrieved from <https://search.proquest.com/docview/1081119777/citation/7A5AA98EDDE3463DPQ/2?accountid=8415>

Sengupta, S. (2012, March 17). The soul of the new hacktivist. *The New York Times*. Retrieved from <https://www.nytimes.com/2012/03/18/sunday-review/the-soul-of-the-new-hacktivist.html>

ADDITIONAL READING

Adams, J. (2013). Decriminalizing hacktivism: Finding space for free speech protests on the internet. *Social Science Research Network*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2392945

Bardas, A., Bell, S., Tian, G., Cain, J., & Oudshoorn, M. (2018). Growing a cybersecurity program: Comparing and contrasting multiple attempts. *Journal of Computing Sciences in Colleges*, 33(5), 186–186.

Bell, S. (2017). Cybersecurity is not just a ‘big business’ issue. *Governance Directions*, 69(9), 536.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2018). Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against Advanced Threats. Retrieved from <https://dl.acm.org/citation.cfm?id=3235132>

Essays, U. K. (November 2013). The problems and solution of hacking computer science essay. Retrieved from <https://www.ukessays.com/essays/computer-science/the-problems-and-solution-of-hacking-computer-science-essay.php?vref=1>

Kostyuk, N., Powell, S., & Skach, M. (2018). Determinants of the cyber escalation ladder. *The Cyber Defense Review*, 3(1), 123-134. Retrieved from <http://www.jstor.org/stable/26427380>

Levesque, M. (2006). *Hacktivism: The how and why of activism for the digital age*. Springer. Dordrecht: The International Handbook of Virtual Learning Environments. Google Scholar.

Lin, H. (2012). Escalation dynamics and conflict termination in cyberspace. *Strategic Studies Quarterly*, 6(3), 46-70. Retrieved from <http://www.jstor.org/stable/26267261>

Moore, D., Shannon, C., & Brown, J. (2002). Code-Red: A Case Study on the Spread and Victims of an Internet Worm. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement* (pp. 273-284). ACM. 10.1145/637201.637244

Sangkya, O., & Kyungho, L. (2014). The Need for Specific Penalties for Hacking in Criminal Law. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4083268/>

Spidalieri, F., & McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: The role of cybersecurity education in US service academies. *The Cyber Defense Review*, 1(1), 141-164. Retrieved from <http://www.jstor.org/stable/26267304>

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *Howard Journal*, 44(4), 4. doi:10.1111/j.1468-2311.2005.00383.x

KEY TERMS AND DEFINITIONS

Activism: A strategy implementing a form of forceful demonstration in order to bring about partisan or societal transformation.

Computer Fraud and Abuse Act: This 1986 Act serves as a modification to existing laws seeking to address issues of deception within the cyber realm. Computer users must receive proper authorization and must not exceed boundaries of authorization.

Criminal Justice System: A system inclusive of law enforcement, the courts, and correctional practices established to control crime and penalize violators.

Cybercrime: Illegal actions conducted via any technological device, which includes hardware and software.

Hacker Culture: A subculture of individuals who abuse vulnerabilities in systems for a common goal.

Hacker Ethics: Principles and ideologies that are shared in hacker culture.

Hacking: Manipulation of a technological device to acquire data unlawfully within a system.

Hacktivism: The combination of ‘hack’ and ‘activism’ to explain the use of technology in the promotion of political or social change.

USA Patriot Act: The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 which granted the federal government increased control in monitoring and interrupting networks in order to counterbalance terrorist attacks.

Hacktivism and Alternative Journalism: The Case of the French YouTube Channel Thinkerview

2

Christophe Emmanuel Premat

 <https://orcid.org/0000-0001-6107-735X>

Stockholm University, Sweden

INTRODUCTION

At the end of 2012, a new YouTube channel named *Thinkerview* was created in France. This channel only contains interviews, between guests and a journalist who does not appear in front of the camera. The frequency of these interviews notably increased between 2013 and 2018. As of 30 November 2018, 126 interviews had been recorded and posted, with durations of between 16 and 140 minutes. The existence of such channels was made possible because of the creation of the YouTube platform in February 2005 (Jarboe, 2011, p. 2), a platform that allowed people to create and edit videos, and make content available immediately, online (Burgess, Green, 2018). Furthermore, it is possible to archive and show old interviews on the platform, thus creating a historical background, which is necessary in order to show a long-term perspective¹. By means of self-generated YouTube channels, new media actors have emerged on the scene, regularly publishing content (Al Nashmi et al. 2017, p. 169 ; Bärthl, 2018, p. 30). *Thinkerview* describes itself as a web channel designed to establish a new model of interviewing. Thinkerview's self-description refers many times to the existence of a "community", as if there is an "anonymous collectivity" (Castoriadis, 1975, p. 433) that supports the programmes and proposes the questions addressed to the guests.

This chapter analyses the positioning and format of a channel that claims to have a close relationship with, and to represent, hacktivists. Here, hacktivism is not seen as a form of criminal manipulation, but rather as referring to the hacker culture, within which people share information and promote full transparency. At the same time, hackers are people who have strong computer skills, and understand the script sources of the Internet (Frichot et al., 2014, p. 8). The interviews are conducted with people who were engaged in sensitive matters, such as the intelligence services, security, hacktivism, investigative journalism, criminal justice, and geopolitics. Lawyers, journalists, and former French Senior Defence staff have been interviewed, and they've provided details about their fields of experience.

What are the characteristics of the YouTube channel *Thinkerview* that distinguish it from classical media in France? In order to describe the work of that channel, it is important to use the concept of Critical Discourse Analysis (henceforth CDA), that focuses on the interactions between the *medium*, the actors, and the scenography. In other words, CDA does not limit itself to the words pronounced by the actors, but analyses the context and social position of the actors. The scenography is also very important, as it creates a specific atmosphere. Scenography is a word borrowed from the theatre, that focuses on performance: "Exploiting the physical power of the performer in the space can illuminate the text, especially if the performers feel confident that they are the primary storytellers" (Howard, 2009, p. 33).

DOI: 10.4018/978-1-5225-9715-5.ch023

In analysing scenography, it is important to focus on the concrete details, such as the construction of the interview, its announcement, and the preparation of the guest. The guests have up to two hours to answer all kinds of questions regarding their jobs, salaries, activism, and political and philosophical backgrounds. Our hypothesis here is that this channel institutionalizes a new critical medium, offering another perspective on the current situation. Thus, these channels can be seen as a form of alternative journalism (Atton, Hamilton, 2008, p. 123), with the aim of uncovering and exposing aspects of contemporary reality that are not covered by classical media. The channels give a voice to investigative journalism and critical thinking, in order to question the dominating discourses. This chapter analyses this “posture” (Panier, 2008, p. 73), in order to see whether the interactions between the guests and the journalist tend to develop a critical discourse on the methods of conducting journalism (Peters, Broersma, 2013). CDA is useful here, as it offers a critical approach to a discourse that pretends to be critical. Hence, it is important to question whether the characteristics of this channel fit its initial intentions.

BACKGROUND

Hactivism is often associated with a form of counterpower, where people get access to secret information. Hacktivists advocate for free access to information and data; they were behind the promotion of free software that does not depend on corporate interests (Krapp, 2011, p. 27). They sometimes denounce the manipulation of information, and propose a new process for evaluating facts and information (Coleman, 2014). A hacktivist is a person who does not accept the expansion of the surveillance society, and who fights for the truth even if this posture contradicts the principles of the State. From the point of view of the security forces, a hacktivist can be a spy, who tries to get access to hidden information while serving the interests of a political power (Guldikova, Santagati, 2000, p. 40). According to Taylor, there was an evolution from hacking activities to hactivism, “an activity that began in the mid-1990s and which refers to the combination of computer-hacking techniques with the real-world, political-activist ethos of new social movements, DIY [Do It Yourself] culture, and anti-globalization protests” (Taylor, 2004, p. 486). Numerous studies have also focused on the instability of cyberspace (Lucas, 2016, p. 17), and the possibilities of manipulating information (Bidgoli, 2009).

At the same time, a hacktivist is also someone who can troll and use non-conventional actions that are criminal (Goode, 2015: 76). The issue of hackers is innately related to cybersecurity issues; hackers are always anonymous, and the frontier between good and bad hackers depends on the context. “More particularly, the hacker community, which forms a strong part of the hacktivist community, is intrinsically linked to the resistance-facilitating potential of technology, challenging established operational and behavioural standards” (Karagiannopoulos, 2018, p. 7). In other words, hactivism is linked with a radical form of freedom of expression, and illustrates a form of electronic civil disobedience (Karagiannopoulos, 2018, p. 49; O’Malley, 2013, p. 140). There can then be a juridical difficulty in determining whether a hacktivist community is simply an outlaw group with illegal behaviours, or whether they are only trying to enlighten the people’s critical thinking. This ambiguity is challenging, as hackers can perceive themselves to be electronic secret agents (Webber, Yip, 2018).

CDA has an interesting perspective, as it focuses on the methodology, rather than on a set of methods. “Settling on a methodology for a particular research project is not just a matter of selecting from an existing repertoire of methods. It is a theoretical process which constructs an *object of research* (a researchable object, a set of researchable questions) for the research topic by bringing to bear on it relevant theoretical perspectives and frameworks” (Fairclough, 2010, p. 225).

MAIN FOCUS OF THE ARTICLE

From this perspective, it is relevant to study the channel *Thinkerview*, a channel that aims to offer enough time for the interviews to tackle all kinds of issues. The selection of the guests, and the scenography, is important, as the performance is presented without any reconstruction. The YouTube channel provides the possibility of following and reacting in real time, but it also allows the interviews to be archived, and provides proof of the popularity of the channel with direct statistics (Kiernan, 2018). The real time effect is all the more interesting, as it creates a form of spontaneity with anecdotes, private jokes, or other details that are usually suppressed in other broadcasts.

THE PROFILE OF THE GUESTS

Statistics on the Interviews

The selection of guests is, of course, the key-concept, as they will be at the centre of the interview. The channel consists of 126 interviews, conducted between January 2013, and 10 December 2018; on occasion, interviews are conducted with several people at the same time, but there is always a hidden journalist guiding the discussions. In total, 171 people interacted with this journalist during these five years, but the number of interviews increased in 2017 and 2018. 46 interviews were conducted between 2013 and the end of 2016, which means that around 64% of the interviews were held in 2017 and 2018². This shows that the channel established logistical routines, and developed a model of interactions that was tested during its first years. In terms of average views on YouTube for each interview, there are around 128,933 views per interview, but the channel's popularity increased from 2017 on, as the average views between 2013 and 2016 were 92,180³. Table 1 presents the main characteristics of the channel.

The gender variable is noticeable, as women constitute only 10% of the interview subjects, as if to say that expertise and knowledge of the world are reserved for men. The gender perspective is not considered by the channel, and feminist issues will not be tackled here as a specific and relevant topic of investigation.

It seems that there is a desire to collaborate with other networks, sharing the ideology of the channel, possessing expertise in domains that are close to the channel's concerns. *Thinkerview's* homepage states, "ThinkerView is an independent group on the Internet, and is very different from most of the think tanks that depend on political parties or private interests"⁴. There is also a quote from Marc Ullmann (1930-2014), a former journalist and essayist who proposed concrete solutions for addressing crises (Ullmann, 1994). The channel presents itself as a tribute to Marc Ullmann; the objectives are then listed as the following: "Test the ideas / discourses by discovering their flaws, their limits. Listen to alternative points of view, in order to broaden our interpretation of reality. Understand the complexity of current and future issues in our world"⁵. The economic model of the channel is crowdfunding, using the platform

Table 1. Characteristics of the channel (2013-2018)

Number of interviews (2013-2018)	Number of individuals interacting with the journalist (2013-2018)	Average number of screen views (2013-2018)	Average duration of each interview (2013-2018)
126	171	128.933	76 minutes

Source: own analysis

Tipeee to avoid any form of dependence (Renault, Ingarao, 2018: 200). Other partners are visible on the page before each interview, they are korben.info, Hashtable (h16free.com), Les Éconoclastes, www.lareleveetlapeste.fr, yogosha.com, sikana.tv, hashtable, yeswehack.com, sixtine.com, lescris.es.fr and captainfact.io. These networks share the same characteristics, as the main authors are anonymous, such as with Hashtable (h16free.com). H16 also published works that focus on current ideologies on climate change. “Maybe I’m going to scare you, but I’m not sure if the information has come to you, I’d like to let you know; given the current situation, the planet is in a bad state, and we’re all going to starve” (H16, 2015, p. 1). H16 is a hacktivist who promotes critical thinking and autonomy. Lareleveetlapeste.fr is an independent publishing house, and a media player. “We are a 100% independent publishing house and media player that self-finance in total autonomy. Our scope is humanist, ecological, and especially antiracist. We finance ourselves with the sales of our books”⁶. This network of partners is cautiously chosen, in order to avoid any kind of dependence, and it is regularly updated. For instance, in the first picture of the interviews from 2017, the partners sikana.tv and captainfact.io did not appear; the network of partners was not large then. The extension of the network of partners afterwards reveals that critical and independent media are encouraged and promoted by *Thinkerview*. Sometimes, during an interview, the journalist asks the community to check some facts on the Internet, to support the discussion. This kind of interaction is very important, in order to avoid misstating facts. In other words, it helps to promote critical thinking as a distinctive feature. The opposition between small circles of people who understand geopolitical issues, and the mass of consumers, is often mentioned in the interviews, such as the one with Pablo Servigne, who promotes concepts such as degrowth⁷.

Networks of Expertise

The guests are invited by the journalist, who uses the alias “Sky”, through his network of contacts. Some guests are recurrent, as the networks allow the journalists of *Thinkerview* to select some favourite guests, such as Pierre Conesa⁸, Alain Juillet⁹, and Olivier Delamarche¹⁰. The association *Les économistes éconoclastes* has also recently started to collaborate with *Thinkerview*. It seems that most guests are people with current or previous experience in domains such as National Defence, Journalism, Finance, Law, Climate change, Astrophysics, or digital issues. The channel has also invited several guests from the army, the intelligence services, and the police. The channel tries to offer an equal voice both to people who fight against mass surveillance procedures, and to people who oppose them on security issues. The case of Alain Juillet is interesting here, as he was a former intelligence agent, and he uses his expertise to explain how the intelligence services contribute to geopolitical relations. The channel is extremely interested in these topics. In the present chapter, the hidden journalist is referred to with the letter J, while the guest is indicated by the letter G. “J: We are going to discuss geopolitics, terrorism, finance, and maybe a little bit about hacking”¹¹. The guests that have expertise feel at ease when they talk about different topics. “J: We begin with Russia; would you be interested in that topic? G: That is a very interesting country, especially with what is going on now, no doubt. J: The Skripal affair, can you say a few words about it? What is your point of view? Is it Cold War propaganda? Do the Russians have something to reproach themselves for? Can you be our spearhead G: The Skripal affair, yes, first of all, it is true that it is...it is an operation that reminds us of the Cold War”¹². The use of ellipsis is worth noticing here, as it is not the country in and of itself that is interesting, but the current situation and the role of Russia in geopolitics. Even in the presentation, the interaction between the expert and the journalist reveals a common interest in describing the geopolitical situation of Russia. This is concrete proof that *Thinkerview* was able to commence its activities thanks to strong networks of expertise (McClurg, 2003).

Favourite Topics or “Killing Darlings”

It is possible to identify several recurrent topics throughout the different interviews. These topics are: geopolitics; security issues; climate change; environmental issues; and the core idea, that of a coming collapse of capitalist societies. The channel promotes different thinkers, and at the end of each interview, the journalist always asks for three books that the guest would highly recommend for a better understanding of the evolution of the world. The agenda is to invite guests, from different ideological horizons, that can discuss the ideology of collapsology. The journalist of *Thinkerview* refers several times to the whistle-blower Michael Ruppert, who predicted the end of economic growth, and a major threat to humankind. Michael Ruppert died a few years ago, and the journalist pays tribute to his documentary on collapse and degrowth¹³. Other distinguished guests share those ideas. For instance, Pablo Servigne, a former engineer who devotes himself to studying the effects of climate change, strongly echoes the idea that collapse is unavoidable. He claims that, unfortunately, most citizens and institutional powers deny this reality, as it would imply changing the economic model of consumption that is based on false ideas of growth. Curiously, other distinguished guests, such as Olivier Delamarche and Charles Gave¹⁴, who are more liberal, also express similar concerns regarding a collapsing financial system. Their main idea is that the European economy is dependent on debt, and that the production of financial liquidity is an immediate reflex of the so-called bureaucrats. These economists belong to very specific networks, such as the *éconoclastes* who cooperate with the *Thinkerview* to organize talks. Some distinguished guests were invited to regularly express their thoughts on geopolitics, such as Pierre Conesa, a former high official from the Department of Defence. As examples, Pierre Conesa shared his expertise on the evolution of Saudi Arabia, on diplomatic relations between France and Russia, and on the war propaganda that we are subjected to (Conesa, 2018).

These guests also have expertise on a dissent discourse regarding the evolution of economic and political institutions in France. *Thinkerview* has also invited some well-known lecturers, such as Jean-Marc Jancovici to talk about the energy crisis, or Bernard Stiegler to discuss the disruption of social links. Jean-Marc Jancovici is an independent lecturer, in the field of energy resources, who has won a large audience for himself. His main thesis is that it is of the utmost priority to invest in decarbonized energy¹⁵. “J: What are the risks, do you think that there is a threat, mmh, that the population is exposed to threats? G: I will begin by not answering your question, and finishing what I previously began with, the only way for me to explain the topic is to use different contact persons [...] If I succeed in convincing a trade unionist, big company executive, or a representative of the economic sector, that my topic is, on the whole, something good for him, then I’ve made a step forward, as he will be able to diffuse a more convincing discourse”¹⁶. Jean-Marc Jancovici thus revealed his lobbying strategy for getting his topic on the agenda. *Thinkerview*’s role is to promote these topics, such as social vulnerability to climate change, and economic collapse and its consequences. As for Bernard Stiegler, he is a philosopher who has devoted his life to studying technological changes (Stiegler, 2018). He has also criticized the development of digital technologies, as he feels they entail the risk of accelerating the destructive forces of the market ideology¹⁷. Here again, the presentation empathizes with the critical role of the guest. “Good evening, Bernard Stiegler, we welcome you to an Internet channel called *Thinkerview*, we are on the air, we welcome you because you are a philosopher, and we noticed that you were deeply interested in topics that we have been discussing for several years, such as the economy, the media, and many other things, including education and, especially, the Internet. How are you doing?”¹⁸

Even if the journalist begins with topics corresponding more with global fields, the strategy is to let the guest talk, and then to ask specific questions regarding the topics, and solutions. Then, Bernard Stiegler continued with a reflection on the American media, and Hollywood, as a machine of desire that produces an idealization of values. He then went on to make a distinction between drives and desires. “Freud explains that to transform drives into desires, it is necessary to educate and transmit a process that operates between the child and his family”¹⁹. The idea was to show that cultural industries destroy the socialization process, and that it is even worse with the digital revolution, as it reduces the possibility of concrete interactions. If the maturation process from drives to desires is broken, there is a risk of devolving to a more primitive state, where individuals do not cooperate. Bernard Stiegler, through his interest in digital objects, thus addressed a critical point of view on the process of civilization. To some extent, he fits in the framework of collapse theory, the main focus of the channel. The questions, therefore, lead the guest to discussing this favourite topic (Nichols et alia, 2010).

The question of digital matters is also one of the expertise zones of *Thinkerview*. The channel invited the current Minister for Digital Affairs²⁰, Mounir Mahjoubi, to talk about how the government is preparing for the digital transition. They always try to invite guests that do not share the same viewpoint on a topic, and this is also the case in regard to attitudes concerning artificial intelligence. For instance, they invited one of the promoters of artificial intelligence, Laurent Alexandre²¹, and a critical voice in the person of Éric Sadin²², a philosopher who presents himself as a strong opponent of the concept of transhumanism. Transhumanism is the belief that, with the development of artificial intelligence, human beings will become a mixture of organic and digital components. In other words, transhumanism puts emphasis on the improvement of human faculties with these technologies. Éric Sadin, for his part, rejects this ideology, which he considers a neoliberal derivative that will model a human being in a very conformist manner. Here, the journalist interrupts guests in a very critical way, when he addresses the questions extracted from the community’s reactions. The confrontation between guests (Éric Sadin opposed Laurent Alexandre, who does not have legitimacy in the field) activates an interaction between all the interviews. It creates a continuity and a historical background, and shows that the channel has the capacity to invite people from opposing ideological backgrounds. One of the characteristics of *Thinkerview* is its ability to take enough time with all its guests in order to deepen the diversity of critical points of view. From this perspective, the scenography is worth studying, in order to analyse how the guests are prepared for the interviews.

THE EFFECTS OF THE SCENOGRAPHY

There is a link between the CDA and the conversational analysis. The conversational analysis focuses on small details (gestures, smiles, interruptions, recurrent interactions), and is illuminating when studying how the guests are prepared, and how they interact with the hidden journalist (Garfinkel, 2002). The aim, here, is to look closely at details that do not seem very interesting at first, but which can offer further insight on our topic. Thus, framing is relevant here, when analysing the interaction between the guest and the journalist in the studio (Goffman, 1966). Language is also used in a very pragmatic way when discussing challenges and solutions to very sensitive problems.

The journalist is behind the camera; he asks questions, makes comments, and reads some questions from the audience that were sent online via social media. The forum on YouTube is used to increase the interaction with the audience. The music played over the opening credits is an intrinsic part of the inter-

view; it can often go on playing for a few minutes until the guest arrives. The music was commented on several times in the channel's forum²³. One of the subscribers wrote the following remark: "When I hear the first notes, I feel transported; I say we will change the world". Another subscriber replied by saying "We will change the world, we are already changing it"²⁴. The music introduces a sense of drama, before the guest comes on the air. The interview is presented as focusing on the performance of the guest, as he or she answers the journalist's questions regarding different topics that are important for the channel.

Presentation of the Channel

The channel's logo is a black swan, which is employed as a symbol of critical thinking, and refers to a theory in statistics regarding the probability of events. Nassim Nicholas Taleb, a writer and PhD in Economics, recently developed this theory. The premise of it is that there is a distance between the reaction of surprise to an event, its consequences, and the reconstructions of its meaning afterwards (Taleb, 2018, pp.1–5). The logo thus possesses a visual identity closely related to the main message claimed by the channel; there is also an anarchistic connotation to the black swan, which is associated with hacktivist values. The engaged hacktivist is believed to be able to predict events in the unfolding crisis of Western societies.

The presentation of the channel is always the same after the opening credits and music case. The journalist introduces the channel, and offers the floor to the guest, so that he or she can describe their activities. The interaction with the guest arouses the attention of the audience. The following example illustrates the sorts of effects that the interaction produces. This is a simpler transcription of conversation analysis (Have, 2007, p. 95) for the forthcoming sequences. "J: Good evening Jérémy Ferrari / G: Good evening / J: We are on the air; can you briefly introduce yourself? / G: Well, my name is Jérémy Ferrari, indeed, I am a humourist and I am on the air (smile) on Sky News / J: On? / G: On Sky News, right? / J: on Thinkerview / G: Thinkerview, Ok, I thought it was more megalomaniac / J: No, no, no, we are a team, we are not megalomaniac; we put our egos aside"²⁵. Here, the interaction is very interesting, as the humourist tries to mock the name of the channel, but at the same time, he does not seem to know its real name. This quick interaction contributes to a better presentation of the channel, even though the journalist goes on with the curriculum vitae of the guest. There is a switch of postures as the guest interrupts the hidden journalist, in order to make him talk about the channel and the objectives. The last sentence ("We put our egos aside") closes the discussion, and the focus shifts to the profile and interests of the guests. Jérémy Ferrari is the second humourist that the channel invited on the air, after Guillaume Meurice in 2017. The presentation of the guest is a part of the scenography, as the journalist justifies the choice of the guest. In the interview with the expert Jean-Marc Jancovici, the main idea was to provide him a voice so that he could put pressure on citizens and political elites: We would like to have your ideas, your opinions on what is going on, the energy, the climate, the carbon tax, all of these small topics (G smiles); how are you doing? G: Well, I am still alive; this is a beginning (G smiles). J: How is it going with your work; is the population sensitive to what you say on the Internet? J: It depends on how we measure the sensitivity."²⁶.

The audience knows that the debate will have some scientific resonance, and the expert is legitimized because he has an unconventional approach to the topic. The question "How are you doing?" is interesting, as most of the guests answer "Not so bad", to illustrate the dramatization of the topics, and the global questions that are dealt with during the interviews. There is a pragmatic intention here, as the

guest expresses how he feels in connection with the topic that will be treated. For instance, Jean-Marc Jancovici's focus is on his message, and how he tries to alert people about the consequences of an over-addiction to some energy sources, such as carbon. Jancovici's concerns are presented as being directly connected to the *repertoire* of *Thinkerview*. This does not mean that the channel approves of his point of view, but it appreciates the critical focus of the guest.

The Analysis of the Backstage

The hidden journalist can sometimes interact in a very relaxed and familiar way with the guest, as was the case with the journalist Isabelle Saporta on 13 March, 2018. Isabelle Saporta has a PhD in Political Science, and she is a journalist and a writer. She began the interview by commenting on what happened before the interview, and how *Thinkerview* contacted her. "J: Good evening, Isabelle Saporta / G: Good evening / J: We welcome you today to a web channel called *Thinkerview*; we welcome you because you are an expert journalist on topics such as agriculture and health; how are you doing? / G: Well, not too bad, in fact, it feels good to be here, I feel pretty good / J: Why "in fact"? / G: Because you are strange, you contacted us in a weird way, didn't you? The phone call was weird, but I liked it; you had to have an instinctive feeling to know that it was going to be OK"²⁷. The guest was referring to the preliminary negotiations conducted before she agreed to come to the channel's studio. She underlined the direct manner the journalist uses to contact potential guests. Sometimes, during the interview, she alluded to details that aren't relevant to the interview. For example, she told the journalist that she forgot to switch off her mobile phone and, when it started vibrating during the interview, she reacted without the audience seeing it. "G: No, no, it is not my daughter (laugh) / J: Here, we have the name of her lover (laugh) / J: Be careful guys, do not let anyone have access to your mobile. G: Are you sure that I do not have to answer; I have to answer, don't I?"²⁸. The mobile phone is useful as a tool for activating the interaction between the journalist and the guest. These spontaneous interactions create a feeling of proximity between the journalist and the guest, as if the guest has accepted the rules of the game, with the possibility of answering or not answering specific questions. It is for this reason that, in the CDA, conversational analysis is adapted to study the digressions and details that appear to be trivial in the interview. Catherine Kerbrat-Orecchioni has studied the creative processes of interactions that occur during a conversation (Kerbrat-Orecchioni, 2005).

During an interview with the pan-African activist Kémi Séba²⁹, the journalist asked the guest to answer a question while he went to the restroom. This received many comments in the YouTube forum. Such a manoeuvre can disrupt the atmosphere, but at the same time, it allows the journalist to change the focus to another question. Kémi Séba is largely regarded as a radical, but his interview reveals a deep concern for the future of Africa. On social networks such as Twitter, many comments were positive, and people were impressed to have the opportunity to get a theoretical background on African issues. For instance, the account "Numidia" (@AmarHaragaa, 27 November 2018) directly commented on the interview: "I just saw the last interview with Kemi Seba by Thinkerview; I thought for a long time that his aggressiveness was bad for his discourse, but it is just amazing here, thoughtful and with such a deep speech"³⁰. Kémi Séba also reacted to the journalist when his enemy's name, Louis Magloire Keumayou, came up. The interview becomes really interesting here, as Kémi Séba performs a sort of multitasking, as he answers the comments of Louis Magloire Keumayou, who was interviewed by *Thinkerview* on 13 September, 2018³¹. Kémi Séba even directly answered a comment posted by Louis Magloire Keumayou on his Facebook page. The multitasking interaction seems to be a characteristic of the channel. The idea is to reveal all sides of the guest, so that they can show who they are in different situations. Implied in

that premise is that a guest thinks that they have the right to discuss a critical topic that others do not have. The quest for legitimacy surrounds non-conventional topics, as if the interlocutors are outsiders who must cultivate an unconventional positioning. There is an emerging hacktivist *ethos* here, where the mainstream media and common topics are denounced as forms of propaganda dominated by a politically correct style.

THE PROMOTION OF A HACKTIVIST *ETHOS*

One of the favourite topics of the channel is the necessity of having an independent media that acts with professionalism and ethics. The journalist often quotes from the Declaration of Munich, which defined the principles of journalism. The interviews can be opportunities to test the guests on their knowledge of this document, which is perceived as an essential part of the duties and rights of journalists. Six journalist syndicates, in six countries of the European community, signed the Declaration of Munich on 23 and 24 November, 1971. In listening to several interviews, it seems as if the channel wishes to consecrate those principles, especially the first one: “Respecting the truth no matter what consequences it may bring about to [the journalist] and this is because the right of the public is to know the truth”³². For the hidden journalist, the Declaration of Munich is a fundamental text that illustrates the duties of journalists. It explains why the journalist of *Thinkerview* invites other alternative journalists and whistle-blowers onto his programme.

The channel aims at confronting *ethos*, a word that denotes a specific posture in the public debate (Charaudeau, 2017). There is a difference, then, between a prior *ethos* (Amossy, 2010, p. 51), and a discursive *ethos* (Amossy, 2010, p. 75). The prior *ethos* reflects the image of the guest before the interview, in other words, their reputation and what is written about them. The discursive *ethos* reflects the performance of the guest, as he or she tries to react to and correct the prior *ethos*. The focus is on the guest, but at the same time, they are reacting to the expressions of the hidden journalist, and sometimes, there is an interaction with the concrete objects present in the studio. The introductory moments that do not seem important as to the quality of the discussion are, in fact, very interesting, as a deal is made between the guest and the journalist. The guest knows the rules of the game, and agrees to enter into this unconventional interview. Catherine Kerbrat-Orecchioni often mentions the interlocution when the speakers interact and exchange views on a topic (Kerbrat-Orecchioni, 1986, p. 10).

“J: Good morning, Laurent Alexandre, thank you for coming to us in Saint-Denis; we begin when you are done with your businessman’s iPhone (G is looking at his iPhone); we are on the air, we would like to correct something about your background. You are not somebody who demands 5,000 euros for conferences; we tested that; you are very accessible on weekends, and you take the time to come from Brussels to Saint-Denis in order to talk with a community of volunteer hackers”³³. In the scenography, the guest is presented as an important person in the field of artificial intelligence, and the journalist begins by nuancing the reputation of the guest. At the same time, he reveals that the studio is in Saint-Denis, and reminds listeners that the people working with *Thinkerview* are volunteers. Laurent Alexandre does not necessarily react to what is said about him; he knows that he is criticized because he advocates more research into artificial intelligence. The discursive *ethos* aims at confirming the prior *ethos*, which means that Laurent Alexandre can declare why it is important to work on those topics. He positions himself on the scene by distinguishing between the people who imagine a nice future, where human beings can be like gods thanks to artificial intelligence, and those who are pessimistic³⁴. “G: We are going to be in an economic, political, social, intellectual mess; we will have great difficulties in seeing where we are

going; we are in a big fog, and many people have certainties that will be contradicted”³⁵. In fact, in the first part of the interview, the journalist comes back to the social perception of the guest; he acts as an investigator who has extracted information from different sources to paint a mental picture of the guest. There is a prior *ethos* that exists in the public space, and on the Internet, but the journalist redefines this *ethos* before allowing the guests to introduce themselves.

In other words, the typical sequence is the following: prior *ethos* / presentation of the journalist / discursive *ethos*. The confrontation of images is a significant part of those interviews, as the idea is to produce a more nuanced image of the guest. The guests do not really identify with the given prior *ethos*; they are able to show, over the course of one hour, how they think and react. The construction of a new *ethos* illustrates a hactivist posture, where people continuously have to question sources, facts, and news. This channel aims to prevent the development of fake news³⁶, which is why alternative journalism is perceived as having a constantly critical attitude.

SOLUTIONS AND RECOMMENDATIONS

- Analyse the background of the YouTube channel to see if there is a regular structure in regard to the information.
- Investigate the scenography to study what the guest wants to say, and how they are guided through the interaction.
- Compare the prior *ethos* in order to the discursive *ethos* to see how the guest perceives their role in the public debate.
- Describe the occasions where the community is referred to, in order to study who follows up the channel.
- Focus on the topics to see whether the alternative point of view is simple due to a form of radicality.
- Integrate a critical forum where facts, sources and news are evaluated. Hactivist channels can contribute to a better critical analysis of media.
- Use long interviews with no montages in order to create an atmosphere of authenticity.
- Produce a critical image of the guest by giving them time to develop their point of view.

FUTURE RESEARCH DIRECTIONS

The objective was to study all so-called alternative media in order to see how they perceive their role, and what types of interviews are prioritized and selected. The combination of CDA and conversation analysis is useful in this, as it is possible to compare the prior and discursive *ethos* that emerges in these kinds of interactions. This research is all the more important, as these small details reveal the objectives and methods of hactivists who reject traditional media. Furthermore, research should be conducted into media that promote alternative facts, or a critical point of view in different fields. Who are the guests? Why are they invited? What does the audience know about their background? A focus on interactions without any montages could be an opportunity to see whether the corrective *ethos* emerges in such a configuration.

The topics of such channels could be studied in detail to see whether the guests bring alternative facts, or a critical point of view on a current debate.

CONCLUSION

2

The channel *Thinkerview* has a central diagnosis on the collapse of the capitalist model of society, and aims to reinforce critical thinking about facts, sources, and interpretations. It invites guests who have a critical point of view, and thus who are not necessarily recognized in the classic media, to appear, even though other official guests can be invited. It is easy to point out the interviews where the hidden journalist shares a form of empathy with the topic. On the whole, the channel attempts to redefine the task of journalism, which is based on critical thinking, independence, and investigation. The ideological references from the journalist are quite obvious when it comes to environmental issues, financial matters, or a mistrust of the classical political establishment. The level of expertise can be quite high, as some scientists are invited to expound on, for example, a novel theory on astrophysics. The objective is to make the channel look like a sort of open university, where it is possible to learn more and check the facts while a distinguished guest talks. The interaction with the anonymous community is quite interesting, as the channel perceives itself as a legitimate medium for critical people. There is a mutual idealization of the channel and the community, as the channel describes a well-informed community, whereas the channel is seen as an alternative mode of information by the majority of subscribers, when the commentaries are analysed.

The ideological part is not the most important one, as the scenography only focuses on the answers and the attitudes of the guests. Long interviews with questions that are not anticipated seem to be the rule; the model of *Thinkerview* has improved in 2017 and 2018, with a larger number of subscribers. The analysis of the attitudes of the guests reveals that the interview confronts, in a systematic way, a prior *ethos* with a discursive *ethos*. In other words, the guests have the opportunity to build a new *ethos*, depending on how they develop their answers. The channel aims to reinforce the links between a community of hackers who think critically about controversial issues. It also offers to some anarchist movements the chance to have a wider audience (Collister, 2014, p. 770).

ACKNOWLEDGMENT

This research was supported by the Department of Romance Studies and Classics (Stockholm University), under a specific research programme on Romance languages, Romling (the number of the grant is SU-165-0030-18 2.1.1). It also received the support of the research network “Language and Power” from Stockholm University (the number of the grant is SU-158A-2.1.1-0075-19).

REFERENCES

- H16. (2015). *Petit traité d’anti-écologie à l’usage des lecteurs méchants*. Paris: Les Belles Lettres.
- Al Nashmi, E., North, M., Bloom, T., & Cleary, J. (2017). Promoting a global brand: A study of international news organizations’ YouTube channels. *The Journal of International Communication*, 23(2), 165–185. doi:10.1080/13216597.2017.1300180
- Amossy, R. (2010). *La présentation de soi. Ethos et identité verbale*. Paris: PUF.

- Atton, C., & Hamilton, J. (2008). Theorizing alternative journalism. In *Journalism Studies: Key Texts: Alternative journalism* (pp. 117–135). London: SAGE Publications Ltd. doi:10.4135/9781446216163.n8
- Bärthel, M. (2018). YouTube channels, uploads and views: A statistical analysis of the past 10 years. *Convergence (London)*, 24(1), 16–32. doi:10.1177/1354856517736979
- Bidgoli, H. (Ed.). (2009). *Global perspectives in information security: legal, social and international issues*. Hoboken, NJ: J. Wiley & Sons.
- Burgess, J., & Green, J. (2018). *YouTube: Online Video and Participatory Culture*. Cambridge, UK: Polity.
- Castoriadis, C. (1975). *L'institution imaginaire de la société*. Paris: Seuil.
- Charaudeau, P. (2017). *Le débat public. Entre controverse et polémique. Enjeu de vérité, enjeu de pouvoir*. Limoges: Lambert-Lucas.
- Coleman, E. G. (2014). *Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous*. London: Verso.
- Collister, S. (2014). Abstract hacktivism as a model for postanarchist organizing. *Ephemera: Theory & Politics in Organization*, 14(4), 765–779.
- Conesa, P. (2018). *Hollywar: Hollywood, arme de propagande massive*. Paris: Robert Laffont.
- Frichot, C., Orru, M., & Alcorn, W. (2014). *The Browser Hacker's Handbook*. Hoboken, NJ: Wiley.
- Garfinkel, H. (2002). *Ethnomethodology's program: working out Durkheim's aphorism*. Lanham, MD: Rowman & Littlefield.
- Goffman, E. (1966). *Behavior in public places: notes on the social organization of gatherings*. New York: Free Press.
- Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. *Popular Communication*, 13(1), 74–86. doi:10.1080/15405702.2014.978000
- Guldikova, I., Santagati, G. (2000). La mondialisation et la culture de participation. *Agora débats / jeunesse*, 19, 31–42.
- Hall, K. (2017). *Creating and Building Your Own Youtube Channel*. New York: Rosen Publishing Group.
- Have, P. T. (2007). *Doing conversation analysis* (2nd ed.). Los Angeles, CA: SAGE. doi:10.4135/9781849208895
- Howard, P. (2009). *What is scenography?* (2nd ed.). London: Routledge.
- Jarboe, G. (2011). *YouTube and Video Marketing: An Hour a Day* (2nd ed.). Sybex.
- Karagiannopoulos, V. (2018). *Living with hacktivism, from conflict to symbiosis*. Cham: Palgrave Macmillan. doi:10.1007/978-3-319-71758-6
- Kerbrat-Orecchioni, C. (1986). 'Nouvelle communication' et 'analyse conversationnelle'. *Langue française*, 70, 7–25.
- Kerbrat-Orecchioni, C. (2005). *Le discours en interaction*. Paris: Colin.

Kiernan, P. (2018). *Language, Identity and Cycling in the New Media Age Exploring Interpersonal Semiotics in Multimodal Media and Online Texts*. London: Palgrave Macmillan UK. doi:10.1057/978-1-137-51951-1

Krapp, P. (2011). *Noise Channels: Glitch and Error in Digital Culture*. Minneapolis, MN: University of Minnesota Press. doi:10.5749/minnesota/9780816676248.001.0001

Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. New York: Oxford University Press.

Marek, R. (2014). *Understanding YouTube: Über die Faszination eines Mediums*. Berlin: De Gruyter.

McClurg, S. D. (2003). Social Networks and Political Participation: The Role of Social Interaction in Explaining Political Participation. *Political Research Quarterly*, 56(4), 448–465. doi:10.1177/106591290305600407

Nichols, J. J., Nichols, J. J., & Schwartz, G. M. (Eds.). (2010). *After Collapse*. University of Arizona Press.

O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity College Law Review*, 16, 137–160.

Panier, L. (2008). Une posture éthique en deçà des valeurs? *Protée*, 36(2), 69–78.

Peters, C., & Broersma, M. J. (Eds.). (2013). *Rethinking journalism: trust and participation in a transformed news landscape*. Milton Park: Routledge.

Renault, S., & Ingarao, A. (2018). Crowdfunding, quand les fans rétribuent les créateurs du web: Spécificités et enjeux du 'Modèle du pourboire'. *Revue Française de Gestion*, 273, 179–203.

Servigne, P., & Chapelle, G. (2017). *L'entraide, l'autre loi de la jungle*. Éditions Les liens qui libèrent.

Servigne, P., & Stevens, R. (2015). *Comment tout peut s'effondrer, petit manuel de collapsologie à l'usage des générations présentes*. Paris: Seuil.

Stiegler, B. (2018). *The Neganthropocene*. Open Humanities Press.

Taleb, N. (2017). Election predictions as martingales: An arbitrage approach. *Quantitative Finance*, 18(1), 1–5. doi:10.1080/14697688.2017.1395230

Taylor. (2004). Hacktivism – Resistance is Fertile? In *The Blackwell Companion to Criminology*. Malden, MA: Blackwell Pub.

Ullmann, M. (1994). *L'État, c'est nous*. Paris: Calmann-Lévy.

Webber, C., Yip, M. (2018). The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. *International Journal of Cyber Criminology*, 230–254.

ADDITIONAL READING

Adam, A. (2005). *Gender, ethics and information technology*. Basingstoke: Palgrave Macmillan. doi:10.1057/9780230000520

Bodford, J. E., & Kwan, V. S. Y. (2018). A Game Theoretical Approach to Hactivism: Is Attack Likelihood a Product of Risks and Payoffs? *Cyberpsychology, Behavior, and Social Networking*, 21(2), 73–77. doi:10.1089/cyber.2016.0706 PMID:28475358

Castoriadis, C. (1997). *The Castoriadis reader*. Oxford: Blackwell Publishers.

Castoriadis, C. (1997). *World in fragments: writings on politics, society, psychoanalysis, and the imagination*. Stanford, Calif.: Stanford University Press.

Cochet, Y. (2005). *Pétrole apocalypse*. Paris: Fayard.

Coleman, E. G. (2013). *Coding freedom: the ethics and aesthetics of hacking*. Princeton: Princeton University Press. doi:10.1515/9781400845293

Deseriis, M. (2017). Hactivism: On the Use of Botnets in Cyberattacks. *Theory, Culture & Society*, 34(4), 131–152. doi:10.1177/0263276416667198

Diamond, J. (2012). *The world until yesterday: what can we learn from traditional societies?* New York: Viking.

Hauskeller, M. (2016). *Mythologies of Transhumanism*. Cham: Springer International Publishing. doi:10.1007/978-3-319-39741-2

Lilley, S. (2013). *Transhumanism and Society: The Social Debate over Human Enhancement*. Springer Netherlands. doi:10.1007/978-94-007-4981-8

Tainter, J. (2013). *L'effondrement des sociétés complexes*. Paris: Retour aux sources.

KEY TERMS AND DEFINITIONS

Artificial Intelligence: Artificial intelligence refers to the creation of an intelligence which is different from human intelligence.” by “The creation of an intelligence, different from human intelligence, usually from computers.”

Collapsology: Set of theories that assumes that the Western societies are about to collapse” by “A set of theories that assume Western societies are about to collapse, and that the global crisis.

Conversational Analysis: Study of the frame of the conversation with specific attention paid to interactive details (interruptions, reformulations).

Critical Discourse Analysis: Field of research that compares the social role of the speakers and the scene of enunciation.

Discursive Ethos: Image of the self that appears during an interview or a discussion.

Hactivism: Political engagement around hacking activities and the access to free and independent information.

Prior Ethos: Image of the self before the discussion (perception of the self by others).

Scenography: Study of the scene frame (concrete location, definition of the setting).

Transhumanism: Ideology that promotes the development of human beings through their interaction with artificial intelligence.

ENDNOTES

- ¹ Les Inrockuptibles, “Entretiens fleuves et sans filtre: que penser de la chaîne YouTube Thinkerview?”, 7 December 2018.
- ² Analysis by the author after compiling all interviews given by the channel. The YouTube channel indicates 130 records with 237157 subscribers.
- ³ As the number of views can always increase, as it is available on the Net, the calculation was made on 10 December 2018.
- ⁴ <https://thinkerview.com/> (Accessed on 10 December 2018).
- ⁵ <https://thinkerview.com/> (Accessed on 10 December 2018).
- ⁶ <https://lareleveetlapeste.fr/produit/manifeste-numero-2/> (Accessed on 10 December 2018).
- ⁷ The interview (23 February 2018) is one of the most important ones in the database with 499872 views as of 17 December 2018.
- ⁸ Interview with Pierre Conesa, 14 September 2018 (Accessed on 17 December 2018).
- ⁹ Interview with Alain Juillet, 7 April 2018 (Accessed on 17 December 2018).
- ¹⁰ Interview with Olivier Delamarche, 11 September 2017 (Accessed on 17 December 2018).
- ¹¹ Interview with Olivier Delamarche, 11 September 2017 (Accessed on 17 December 2018).
- ¹² Interview with Alain Juillet, 7 April 2018 (Accessed on 17 December 2018).
- ¹³ The documentary was made by Chris Smith in 2009 about the theories of Michael Ruppert.
- ¹⁴ Interview with Olivier Delamarche, Charles Gave and Pierre Sabatier (3 April 2018, Accessed on 17 December 2018).
- ¹⁵ Interview with Jean-Marc Jancovici, 14 December 2017 (Accessed on 10 December 2018).
- ¹⁶ Interview with Jean-Marc Jancovici, 14 December 2017 (Accessed on 10 December 2018).
- ¹⁷ Interview with Bernard Stiegler, 17 January 2018, (Accessed on 10 December 2018).
- ¹⁸ Interview with Bernard Stiegler, 17 January 2018, (Accessed on 10 December 2018).
- ¹⁹ Interview with Bernard Stiegler, 17 January 2018, (Accessed on 10 December 2018).
- ²⁰ Interview with Mounir Mahjoubi (31 October 2017, Accessed on 17 December 2018).
- ²¹ Interview with Laurent Alexandre, 8 November 2017 (Accessed on 10 December 2018).
- ²² Interview with Éric Sadin (8 November 2018, accessed on 10 December 2018).
- ²³ Introductory music (Accessed on 10 December 2018).
- ²⁴ Introductory music (Accessed on 10 December 2018).
- ²⁵ Interview with Jérémy Ferrari (27 November 2018; 127721 views as of 13 December 2018). The English translation is by the author.
- ²⁶ Interview with Jean-Marc Jancovici, 14 December 2017 (Accessed on 10 December 2018).
- ²⁷ Interview with Isabelle Saporta (13 March 2018, accessed on 10 December 2018).
- ²⁸ Interview with Isabelle Saporta (13 March 2018, accessed on 10 December 2018).
- ²⁹ Interview with Kémi Séba (21 November 2018, accessed on 10 December 2018).
- ³⁰ <https://twitter.com/AmarHaragaa> (Accessed on 10 December 2018).
- ³¹ <https://thinkerview.com/sankara-francafrique-cfa-ou-va-lafrique/> (Accessed on 10 December 2018).
- ³² <http://www.mediawise.org.uk/european-union/> (Accessed on 10 December 2018).
- ³³ Interview with Laurent Alexandre, 8 November 2017 (Accessed on 10 December 2018).
- ³⁴ Interview with Laurent Alexandre, 8 November 2017 (Accessed on 10 December 2018).
- ³⁵ Interview with Laurent Alexandre, 8 November 2017 (Accessed on 10 December 2018).
- ³⁶ <https://www.youtube.com/watch?v=pCd0oAJlxyI> (Accessed on 10 December 2018).

Drifting on the Web

Lila Luchessi

Universidad Nacional de Río Negro, Argentina & Universidad de Buenos Aires, Argentina

Ana Lambrecht

Universidad Nacional de Río Negro, Argentina

INTRODUCTION

The massive expansion of social media networks makes it necessary to study them from an interdisciplinary point of view.

In Argentina, the use of digital social networks led government agencies to share through them public and management information, substantially increasing their presence in these new platforms.

From an administrative point of view, social networks are thought of as tools which facilitate access to public information to the citizens. On the one hand, they give everyone easy access to public information, and, on the other, they shine a light of transparency and effectiveness to the activities of public agencies. These features make them engaging for the members of the administration.

The benefits derived from their use seem clear and numerous. Nevertheless, the actions performed within them produce certain legal conflicts. To be able to use them, you must agree to a contract with pre-established clauses which might a priori override certain principles ruling the Public Administration of Argentina, and of other countries protecting their citizens with data protection acts.

In that respect, this work aims to make a communicational-legal analysis which particularly focuses on how the State uses social networks within the legal framework of Personal Data Protection Acts, and whether it enforces compliance with the law by those entities which have the right to freedom of expression, but are not responsible for protecting the right of privacy of the citizens.

Analyzing the use of Social Networks by State agencies in Argentina from a legal perspective is quite relevant, because of the countless facets deriving from that issue, each of which requiring an individual and detailed analysis. Therefore, and in view of the contractual terms and conditions users accept when using digital platforms, a comprehensive analysis will be made as to the obligation of the State of protecting the citizens' personal data, and the legal framework governing such case.

To that aim, we will analyse the presence of public agencies on the social networks, the information they provide to them, and the potential lack of legal protection of the citizens.

The analytical method is to study certain cases in which public entities have shared information on the networks, while at the same time collecting sensitive information about the citizens. The research variables refer to the publicity of public information and the right of privacy.

The cases chosen were the Facebook pages of the National Agency of Social Security (ANSES, in Spanish), the Government of the City of Buenos Aires, and the Ministry of Education of Argentina.

SOCIAL NETWORKS

2

When we talk about “social networks”, it is important to consider them as a wide concept and a tool with countless facets. Before examining in detail the digital platforms, which enable interactions among users, it should be said that networks are previous to the appearance of digital technologies; that communities, are articulated in a relational manner, that they are centrally based on connections, and that interactions are their fundamental feature.

Passing now to the analysis of platforms, Fernando Tomeo refers to them as “...Internet Sites (digital platforms), which enable users to show their profiles, upload photos, tell personal experiences, chat with friends, and, in general, share and exchange all types of contents (information, opinions, comments, photos, videos)” (Tomeo, 2010) (Own translation).

Then, it should be possible to say that these virtual sites, which are a vehicle to social communication, allow people to share and exchange contents and enter into free relationships with other users, which enable them to connect and interact on the Internet. In this way, we could refer to convergent communities in digital interaction.

To a greater or lesser extent, platforms increase their popularity and their function is no longer reduced to being mere communication channels. Their use may be analysed from many perspectives: from the technical point of view, as to the incalculable amount of information circulating; from the economic point of view, as to the continuous amount of money these data and information generate; from a psycho-social point of view, as to the sense of belonging and omnipresence they create when people engage with other people -known or unknown to them- from around the world, whether on a social, work-related or personal level, among others.

The power and growth of these virtual platforms focuses on the storage of information and personal data. This also enables them to create algorithms to determine the preferences of the users, and to develop specific segmentations based on consumption patterns. (Tomeo, 2012).

The legal relationship between the user and the social network is established through a contract of adhesion. The user agrees to a set of clauses unilaterally established by the company, without having the possibility of negotiating any of the terms and conditions stipulated.

Generally speaking, and specifically in relation to the contractual terms and conditions, most of the social networks have similar clauses. For the purposes of this analysis, we will analyse the terms and conditions laid down by Facebook (Facebook, 2019) and Twitter (Twitter, 2019), since they are the virtual platforms with more presence of official State accounts.

Facebook, for its part, has become the social network with the highest number of users. According to Digital 2019 Global Digital Overview, it has more than 7.77 billion users and 2,200 million daily active users (We Are Social, 2019). That makes of Facebook the most profitable social network in the world, with a market value of more than \$ 400 billion (ElEconomista.com, 2019).

The increasing use and presence of this social network in Argentina has made the company set up Facebook Argentina S.R.L. in 2011, which currently has more than 20 million monthly active users within the country. This number is a clear evidence of how relevant this network has become in Argentina in terms of scope and expansion. Since the number of users accounts for more than half of its population, Argentina is among the 20 countries in the world with the higher number of users, and second in the region after Brazil (Fernandez, 2019).

The power and growth of this virtual platform focuses on the storage of information and personal data. This also enables it to create algorithms to determine the preferences of the users, and to develop specific segmentations based on consumption patterns. (Tomeo, 2014)

By contracting Facebook, a legal bond is established in which the user accepts a contract of adhesion made out of various supplemental documents where the general terms of service are laid out. Some of them are:

- Statement of Rights and Responsibilities of the Users
- Data Policy, which describes the type of information collected by the social network and how that information will be used and shared
- Payment Terms, which lays out the provisions governing payments through the platform.
- Provisions related to Advertising Policies, guidelines applied to Promotions and Brand Resources, Page Terms and Conditions.

Each of these documents is accepted by the user when creating a Facebook account. All it takes is a “click”, and users might not be aware -many times- of the risks entailed.

The Statement of Rights and Responsibilities (SRR), lays down the general guidelines on the use of the data assigned to the virtual platform, licenses granted, legal aspects and applicable jurisdiction.

By accepting the SRR and the supplemental documents, the user:

- Automatically agrees to the clauses laid out on them.
- Gives consent to having his/her personal data transferred to and processed in the United States, according to section 16.1 of the Statement.
- Grants Facebook a worldwide non-exclusive, transferable, sub-licensable and copyright-free license to use any content with intellectual property rights posted on Facebook. The license ends when the content is erased, unless it had been shared with third parties who had not deleted it.
- Provides instructions to report illegal contents, fake profiles or false advertising, which are deleted after previous analysis.
- In relation to intellectual property rights, it must comply with the applicable laws, and more specifically, with the Digital Millennium Copyright Act and the Video Privacy Protection Act of the United States.
- Facebook establishes unilateral limited liability.
- It submits itself to the jurisdiction of the United States District Courts for solving any claim or dispute.

When signing up for Facebook, the user accepts all the above-mentioned clauses and, at first glance, he/she should comply with them without being able to challenge them.

As to Twitter, it is a social network with an important number of followers and it has become another leading social network on the Web, thanks to the users it adds every day, its monetary revenue and its market value. This social network has currently around 326 million users across the world (We Are Social, 2019).

Broadly speaking, Twitter and Facebook have quite similar Privacy Policies and Terms and Conditions, and their contracts do not hold major differences.

The terms of service laid out by Instagram, Snapchat and Youtube are also similar to the ones developed above.

According to the basic principle of contract law, the most relevant clauses of the contract of adhesion to social networks which were mentioned before are legally-binding for the parties, since there has been an acceptance by the user.

THE STATE ON THE WEB

2

Having defined the concept of social networks and analysed the general clauses established by their contracts of adhesion, we have now a general outline of the functions played by these virtual platforms. On that principle, we will now analyse how public administrations, in any of their forms or levels, make use of them.

This phenomenon has not gone unnoticed for scholars and academicians who have devoted themselves to analyse it, trying to understand, on the one hand, the need of the States to be part of these networks and, on the other, the social, political and economic impact their use brings about.

Many studies have been made in relation to the impact of the use of social networks by public administrations. Among them, we could mention Calderón, 2008; Criado and Rojas, 2012; Valenti and others, 2015; Criado and others 2015. Broadly speaking, these works point at the impact the use of social networks has had in the performance and development of management in public administrations, putting special emphasis on the way in which the managerial operations of the States who want to show signs of transparency, efficiency and efficacy have changed.

All of them agree that the emergence of virtual platforms has brought inestimable benefits to the sphere of the State. Furthermore, they share the idea that public administrations have the compelling need of having a presence on the Web through the virtual platforms.

Their use is key in the government's agenda: from an administrative and democratic point of view, they become essential not only for the citizens but also for the administration itself.

By having a presence in the social networks, the State conveys an image of transparency, trustworthiness, efficacy and management achievements, which is shown openly, in a direct manner and with a social perspective. That presence sheds light on the policies that the government and the State put into practice, which has a very positive impact on a social and political level and adds to the development of a sustainable Estate.

Far from the obscurantist view of public management, which was detrimental to the State both inwards and outwards, publicity on digital networks has drawn citizens closer and generated respect and trust in terms of institutionality, a concept with negative connotations before their use.

Virtual platforms have a vast spectrum of possibilities: they can be used to publish judicial rulings, public works presentations and services available for the citizens, and they may also become a powerful communication tool which may determine an electoral victory.

The 2008 United States election is a clear example of this: Barack Obama presidential campaign took place almost exclusively on the social networks. This allowed him to reach the White House with the largest share of voters, who had been previously engaged in the virtual platforms with the highest number of users (Carr, 2008).

To illustrate this point, we could mention some countries whose States are active users of social networks, something which has become quite significant to them. That is the case of the United States; the White House official Twitter account twitter.com/WhiteHouse, has 17 million followers. Spain, for its part, is registered under the official account of the Spanish Government twitter.com/desdelamoncloa, which currently has more than 0.5 million followers. In the same way, the State of Colombia is registered as a user since 2011 under the official account <https://twitter.com/infopresidencia>, which has more than 700,000 followers.

All the above-mentioned countries have an official presidential account, and also official accounts for each of the several agencies that make up their Public Administrations. Those accounts make an important communication and management work to have presence in the social media, clearly aiming to be part of a reality they have to involved in.

The number of followers or friends of each of those accounts is quite significant and they are continuously growing. That fact shows the importance of these platforms and how relevant it is for the States of different countries to increase their presence and posting frequency on them.

Presence in the social networks is nowadays so interesting that even the Judiciary has been involved in certain affairs related to accounts considered to be public. That was the case of the American Federal Justice when it recently ruled that the President of the United States had violated the First Amendment of the American Constitution.

Donald Trump had blocked a user from his Twitter account. The Court considered that when it comes to the President, his account is a public forum whose restriction would constitute discrimination that violates the applicable legislation (Kludt, 2018). President Donald Trump Twitter account (@realDonaldTrump) has currently more than 56 million followers.

Through its different agencies in all levels of the administration, the Argentinian State has also become a permanent and very present user of virtual platforms such as Facebook, Twitter, Instagram, and even Snapchat.

The new forms of communication have outdated the old access methods to public information, justice and any other management action performed by the State agencies, since the number of government entities has increased.

The Argentinian Government spends an important amount of the National Budget in the management and control of the social networks. In that sense, it created the Citizen's Bond Committee, dependent on the Presidential Secretariat of Public Communication.

The entity has 100 employees whose role is to design communication strategies in the social networks.

In 2016, the Government assigned to that Committee more than 160 million Argentinian pesos from the National Budget. The argument employed is the need of communicating acts of government and the direct bond that the use of virtual media establishes with the citizens. (Recalt, 2016)

This gave rise to multiple controversies (Alfie, 2016). In spite of them, it is possible to say that, according to Section 11, subsection 2), paragraph c) of the Personal Data Protection Act No. 25.326, and pursuant to its powers, the State is entitled to share with its own agencies all data derived from State Entities.

In Facebook, the official account of the Presidency of the Republic of Argentina is <https://www.facebook.com/casarosadaargentina/>, and it has more than 1.6 million users. In Twitter, the official account is <https://twitter.com/CasaRosada>, and, as the Facebook account, it has numerous followers.

Effectively, the examples mentioned allow us to see the presence of the State in the social networks. We have taken those two accounts in a descriptive way, since there are multiple accounts from State Agencies dependent on the National, Provincial and Municipal branches.

In effect, the Argentinian State is a user of social networks. To be one of them, it had to accept the contracts of adhesion analysed in the previous section. By accepting them, the adherent, in this case, the State, creates a legal bond that brings about unfavorable legal consequences for the State and has an impact on third parties, or more precisely, on the people governed by it.

In that sense, it is also possible to debate whether the State should abide by the Consumer Protection Law No. 24.240, whether it should be treated as a regular consumer, or whether a new legal figure contemplating the special nature of this user should be created. Nevertheless, the topic is beyond the aim of this work. We will only say that currently, according to the applicable law and since we are in the presence of a legal void, the State should be considered as a user or a consumer as described in the above-mentioned law¹.

It is not possible to find specific legislation that can be applied to the use of social networks by the State. Therefore, it will be necessary to explore all the legal corpus to establish which laws may be applied in that case.

Generally speaking, when comparing the legislation of several countries, it is only possible to find general guidelines on the use of social networks by the State. At first sight, it is not possible to find laws which establish terms and conditions with the companies owning virtual platforms that acknowledge a priori that the user accepting the contract is not an individual but the State, through its agencies. Such user requires concrete and specific laws which allow it to make an adequate use of the networks, complying at the same time with its applicable legislation.

Among other cases, we could mention Mexico, which has a Handbook of Policies and General Guidelines on the use of Virtual Social Networks by the Government of the State of Mexico (Gobierno del Estado de México, 2010), which establishes clear policies as to the general guidelines to be followed by the State when using social media. This handbook was designed to set goals to make the most of all the benefits provided by the social networks.

Countries such as Dominican Republic also have general guidelines related to the use of social networks by the Public Administration, which are laid down in the Policies of Social Networks Accounts of the Government. They establish certain strategies to be taken into account in the use of virtual platforms, and certain policies for them to be used correctly.

With regard to Argentina, the country does not currently have a legislation which particularly rules the issues being analysed. Even so, there have been important and paradigmatic changes lately in relation to communication strategies. In fact, several entities to modernize the Public Administration have been created, which shows a clear intention of the Government of having a strong virtual presence in the social media.

In the legal aspect, it is only possible to find that according to Resolution No. 13345/2017 of the National Directorate of Digital Content, there has been established a control regime which is only applicable to the opening and registration of social networks accounts by State agencies. The accounts owned by officials and employees of the National Government are not included.

Therefore, all the legislation ruling the matter is not sufficient to rectify the fundamental issue: that the State is accepting a contract of adhesion with different companies which collect personal data, whether or not the service is free, and that it ends being subject to certain clauses as if it were an ordinary individual, without considering its institutional peculiarities and the laws governing the public administration.

ON PERSONAL DATA PROTECTION

When referring to personal data, it is impossible not to mention the description and special considerations included on Section 2 of the Argentine Data Protection Act No. 25.326, which defines them as “information of any kind referred to certain or ascertainable physical persons or legal entities.” This

Act also references to sensitive data, making a difference from the above by considering them “personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior.”

For the purposes of this article, this difference is not substantial, since when talking about personal sensitive data we should always take into consideration the special and particular features of each case.

The issue of personal data protection appears as one of the fundamental factors when it comes to using social networks. As analysed in the terms of service, by accepting a contract of adhesion to the platform, the user gives consent to have his/her data transferred to and processed in the United States. Pursuant to Section 16 of the Facebook Statement: “Special Provisions Applicable to Users Outside the United States. We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States: 1.-You consent to having your personal data transferred to and processed in the United States...”

In Argentina, the Personal Data Protection Act No. 25.326 defines on Article 2 that personal data are: “Information of any kind referring to defined or definable individuals or corporations.”.

This law stipulates the minimum guidelines as to the quality of the data received. Those data must be true, adequate and pertinent, and they could only be used for the purpose or object they have been collected for. Their processing is only allowed after the free, expressed and informed consent of their owner.

In the same way, in relation to data assignment and international transference, Articles 11 and 12 of the above-mentioned law establish, respectively:

“Art. 11.- (assignment). Personal data subject to processing may only be assigned to comply with purposes directly related to the lawful interest of both assignor and assignee, with prior consent of the data owner...”

“Art. 12.- (international transfer). 1. Transfer of personal data of any kind to any country or international or supranational organization is hereby forbidden if adequate protection is not provided”.

Indeed, we find ourselves in a situation in which the State, who should guarantee the enforcement of the laws which comprise the Argentinian legislation, not only does not guarantee the enforcement of the laws, but also deliberately violates them.

It is clear that this occurs because of the eagerness to use new communication mediums, have direct contact with the citizens without the mediation of the press and implement new ways of Public Management.

The State, as the most powerful organization in society, continually collects data from the citizens related to every aspect of their lives. Within the mass of data that constitute its base, it is possible to find information ranging from personal information to racial or ethnic origins, passing through issues referred to health, political affiliation or personal assets.

This is a very sensitive aspect and it requires a deeper study. The State, in all its branches and levels, is the most important data collector. The amount of information it collects from the citizens is incalculable. It stores a person’s date of birth, level of education, localization, medical history and even his/her criminal record.

In this context, by using the social networks and posting content on them, which always relates to the citizens, the State is not only making use of the important benefits provided by the platforms, but it is also assigning all those data to a foreign company allowing it to use them in an indiscriminate way, without any kind of restrictions or accountability.

The excessive violation of the data protection laws by the State has many steps. The first step is the collection of data, the fact of not informing the owner about the processing or destination of those data, and the absence of the tacit and expressed consent required by the legislation. Then, there comes the transfer of data to a foreign company to have them processed in a foreign country, without the owner's expressed consent. Finally, the owner ignores the treatment the collected data will receive and who has access to them.

To the situation described, an aggravating factor should be added related to the entities to which the State accepts to transfer all its citizens' data. They are companies which develop their economic activities and get astronomical amounts of revenues due precisely to the traffic, processing and reception of the data continually assigned to them by the users.

Since there is no distinction between the individuals and the entities providing information when the contract is signed, the Argentinian State, as well as all the States signing up to these social networks, submit themselves to the rules of another State, without having the possibility of exerting influence over their making or enforcement.

Nowadays, the transaction of personal data has increased exponentially. So much so that it is considered to be one of the most important businesses of the last decades. Taking this situation into account, and given the compelling need of giving more protection to personal data, the European Union enacted the General Data Protection Regulation (GDPR). This Regulation increases data protection and establishes clear stipulations as to their processing and transference. It is expected that the legislation of the rest of the countries will also increase data protection and establish severe sanctions in case of infringement.

Argentina has been one of the first countries in the region to include in its legislation the issue of data protection, understanding their importance and the need to protect them. Currently, the process begun by those guidelines is being reinforced. For that reason, the country has proposed certain legal amendments which tend to strengthen data protection in accordance with the GDPR.

In that sense, certain countries of the region, such as Chile and Brazil, have proposed significant changes in their personal data protection laws. In line with the European legislation, the Latin American countries have considered that increasing data protection is quite relevant within the current context of massive access to computers.

Nevertheless, the progressive legislation which guarantees the protection of data is not consistent with the daily processing of data in the social networks accounts of the public agencies. There, it is possible to find posts showing pictures of minors, addicted and vulnerable people, and convicts, along with their personal data to have them identified more easily. As said before, all those data are freely transferred and assigned to the social network in which those pictures are shared.

Therefore, it would be important for the controlling bodies to exert the necessary control mechanisms to allow the Argentine State to enforce the applicable laws that have been promoted and enacted by itself.

This analysis focuses on the violation of the protective data protection laws by the State in spite of its own nature within the realm of the rule of law and its inherent obligation to protect every aspect of the lives of the citizens it governs, including their personal data. The analysis would be very different if we were dealing with a private company or the media themselves, since neither of them has the same obligations of the State.

ACCESS TO PUBLIC INFORMATION AND THE DUTY TO COMMUNICATE

The American Convention on Human Rights, or Pact of San José, Costa Rica, was approved and enacted by the Argentinian Congress by Law No. 23.054 on September 5th, 1984. With the Constitutional Reform of 1994, it was incorporated to the Magna Carta and enjoys constitutional status through Article 75, Subsection 22.

Its articles protect the citizens' right to privacy, and the rights of freedom of expression, conscience, reply, association and religion.

In its article 11. 2, it stipulates that: "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation".

In this sense, the fact that the Argentinian State accepts a contract without being able to negotiate the clauses with the companies imposing it, which submit its regulation to the laws of another State, poses a risk in the compliance of the constitutional legislation.

The State is obliged to provide the necessary information for the citizens to exercise their rights. But the choice of doing so through virtual platforms developed by oligopolies, which set regulations to solve any claim or dispute in a foreign territory with laws of its own, may put the guarantees of the citizens against the wall to favor multimillion-dollar businesses and geopolitical interests that do not represent them.

The consultations, comments and horizontal interactions that take place when posting on the state agencies accounts allow to keep a record of citizens with specific characteristics.

In the cases analysed for this work, we have found pictures, videos and testimonies of citizens regarding the services provided by each of the state agencies.

In this way, elderly people declare the amounts and taxes that they pay for loans asked to the Social Security system, minors are exposed in photographs taken in schools dependent on the Ministry of Education, and residents of the City of Buenos Aires appear in pictures illustrating public works, services and activities performed by the autonomous government of the City.

On the other hand, although most of those people are users of these platforms, and therefore their personal consent exempt the companies from responsibility, there have been cases of arbitrary censorship: they are the result of the application of rules derived from non-universal cultural guidelines, and constitute examples of intervention over the cultures, practices and habits of other people.

This arbitrariness affects many citizens who use the social networks and, in the worst scenario, the assignment of data allows the companies to have access to sensitive information related to ideological stances, religious beliefs, health condition, and any other aspect compromising the privacy of the citizens.

It can also be seen that when people make claims through the Web in relation to identity records or small-scale data thefts, upload transaction forms or have access to public proceedings, the traces of that information might also be collected to be processed in ways which are not specified in the contract proposed by the companies managing the platforms.

Then, in the trajectory of the user from the agency account to its web site, more information is assigned which might be used in an arbitrary way. The risk of inequity and failures in data processing have already had negative results, such as arbitrary detentions derived from facial recognition, or purchasing of information by certain corporations aiming to obtain ideological stances or health condition of certain people, all of which emerging from posts made on the social networks.

CONCLUSION

We are faced with a reality in which presence in the virtual media -not only for individuals but also for the States- is essential. Nevertheless, the acceptance of a contract of adhesion established unilaterally creates an undeniable asymmetry of rights and obligations.

There is an increasing number of States around the world which use the social networks as communication mediums, because they have understood that there has been a change in the forms of communication, and that using virtual platforms gives them a sense of transparency, efficacy and effectiveness. That use also allows them to avoid the mediation of the press and guarantees direct access to the segments aimed at without the intervention of third parties.

In this context, the existing legislation in many countries, including Argentina, is limited to lay down mere guidelines on the use of social networks, without addressing the main issue: the adhesion to a contract pre-designed by a company, which creates a legal bond with the State which has unfavorable legal consequences for it.

In Argentina, the State -by adhering to the social networks- systematically violates the Personal Data Protection Act. The paradox is that, according to the legal framework regulating its actions, the State should be the one to enforce the law and create the necessary mechanisms to duly protect the personal data of the citizens over which it governs, which should be protected under the principles of the international treaty that protects human rights and enjoys constitutional status.

In this scenario, the State does not have clear processes, public policies and regulations on the use of social networks, not only regarding their administrative use, but also as to the conditions of use and processing of data it should be subject to.

The control mechanisms established by the State should be firstly aimed at adjusting the legal system to the current reality. Furthermore, it is most relevant that the State, under its legal authority, builds the necessary negotiation processes with the companies owning virtual platforms, to design bilateral contracts with clauses and stipulations applicable to the State as such.

The State has the obligation of activating its own control mechanisms through the appropriate entities in order to exercise control over data protection, violation of intellectual property rights, access to information and, basically, the right to privacy.

This should be done not only to protect itself, but also to justify its own purpose of existence: to protect, guarantee and safeguard the protection of the rights of each and every citizen.

REFERENCES

- Alfie, A. (2016). Campañas Personalizadas. *Clarín*. Available at https://www.clarin.com/politica/usaran-confidenciales-anses-publicidad-oficial_0_HyY9MSEO.html
- Balbín, C. (2011). *Tratado de Derecho Administrativo*. Buenos Aires: La Ley.
- Balestra, R. (1988). *Manual de Derecho Internacional Privado*. Buenos Aires: Abeledo Perrot.
- Bauman, Z. (2003). *Comunidad. En busca de seguridad en un mundo hostil*. Madrid: Siglo XXI.
- Biocca, S., Feldstein De Cardenas, S., & Basz, V. (1997). *Lecciones de Derecho Internacional Privado*. Buenos Aires, Ed. Universidad.

Carr, D. (2008). How Obama Tapped Into Social Networks' Power. *The New York Times*. Available at <https://www.nytimes.com/2008/11/10/business/media/10carr.html>

Cassagne, J. (2007). *Tratado de Derecho Procesal Administrativo*. Buenos Aires: La Ley.

Castells, M. (2001). *Internet y la sociedad red*. Academic Press.

Chapman, A. (2001). La propiedad intelectual como derecho humano. *Boletín de Derechos de Autor*.

Criado Grande. (2012). *Las redes sociales digitales en las administraciones públicas iberoamericanas: retos y perspectivas de futuro*. CLAD.

ElEconomista.com. (2019). *Facebook CL A*. Available at <http://www.eleconomista.es/empresa/FACEBOOK>

Farina, J. (2000). *Defensa del consumidor y del usuario*. Buenos Aires: Ed. Astrea.

Fernandez, R. (2019). *Países con más usuarios de Facebook a nivel mundial 2019*. Available at <https://es.statista.com/estadisticas/518638/ranking-de-los-20-paises-con-mas-usuarios-de-facebook-a-nivel-mundial/>

Fernandez Delpech, H. (2012). *Manual de Derecho Informático* (A. Perrot, Ed.). Buenos Aires: Academic Press.

Jenkins, H. (2006). *Convergence Culture. La cultura de la convergencia de los medios de comunicación*. Barcelona: Paidós.

Kludt, T. (2018). *Trump no puede bloquear usuarios en Twitter, ordena una jueza federal*. Available at <https://cnnespanol.cnn.com/2018/05/23/trump-no-puede-bloquear-usuarios-en-twitter-ordena-una-jueza-federal/>

Lorenzetti, R. (2003). *Consumidores*. Buenos Aires: Rubinzan Culzoni Editores.

Luhman, N. (1995). *Social Systems*. Stanford University Press.

Marx, K. (2005). *Elementos fundamentales para la crítica de la economía política I (Grundrisse) (1857-1858)*. Siglo XXI.

Palazzi, P. (2003). *Principios para la protección de datos personales en la nueva ley argentina en Revista Derecho Informático, No. 3*. Santa Fe: Editorial Iuris.

Palazzi, P. (2017). Transferencia Internacional de datos personales. Nueva Regulación de la Dirección Nacional de Protección de Datos Personales. *La Ley*, 81(33).

Recalt, R. (2016). *El gobierno gasta \$160 millones al año en redes sociales*. Available at <http://www.perfil.com/politica/el-gobierno-gasta-160-millones-al-ano-en-redes-sociales.phtml>

Stiglitz, G. (1990). *Protección Jurídica del Consumidor*. Buenos Aires: Depalma.

Tomeo, F. (2010). *Las redes sociales y su régimen de responsabilidad civil*. Buenos Aires: La Ley.

Tomeo, F. (2014). *Redes Sociales y Tecnologías 2.0*. Buenos Aires: Astrea.

We Are Social. (2019). *Digital 2019 Global Digital Overview*. Available at <https://www.slideshare.net/DataReportal/digital-2019-global-digital-overview-january-2019-v01>

ENDNOTE

- ¹ Law No. 24.240, section 1: “... a consumer is a physical person or legal entity which acquires or uses goods and services as a final consumer, whether freely or in an onerous way, for their own benefit or for the benefit of their own household or social group.”

Cyber Crime Regulation, Challenges, and Response

Sachin Tiwari

 <https://orcid.org/0000-0001-5526-129X>

Jawaharlal Nehru University, India

INTRODUCTION

The cyberspace emergence has created a new reality with transnational connection providing a venue for growth and also for contestation (Chourci, 2012). Defining the characteristics of the cyberspace includes various attributes such as; diffusion of power, ease of accessibility, low cost of entry, attribution, i.e., anonymity (Nye, 2011). The cyber domain position is characterized as a “transnational domain for information and economic exchange, which contemplates the transnational nature of the internet and the problem of global governance” (Kiggins, 2014). Definition of cybersecurity has constantly shifted to reveal the growing number of threats and new areas affected by the attacks. The case of UNGA resolution 53/70 where the modification of definition from the phrase ‘may adversely affect the security of the state’ in 1999 to ‘may adversely affect States in both civil and military fields’ in 2002 reflects the change in definition due to evolving nature and increased threats (Radu, 2014). Effectively, cybercrime was seen majorly as a technical issue, however, the course changed with the increase in incidents and the need for regulating it. The effective cost of cybercrime has increased with sophisticated tools being employed for a criminal purpose especially with the rise of ransomware as an industry. The concern arises from the fact that the average cost for the enterprises was \$11.7 million of cybersecurity due to cybercrime, with an increase of 27.4 percent each year (Accenture, 2017). Platforms like Convention on Cybercrime in 2001, World Information Society in 2003, have pushed for a ‘global culture of cybersecurity’ and laid the foundation for the effective policymaking at the international, regional, and national level. Moreover, the international scenario is constantly molded by the sophisticated cyberattacks, global geopolitical shifts, and social media empowered by political move with the divergent position of the states. The variance is visible in the cyber legislation with varying definitions, development with one paternalistic group of countries advocating state sovereignty while other members promoting freedom of internet and role of private companies

In this perspective, the article aims at presenting and analyzing the state of the growing threat of cybercrime and the resultant laws being enacted at the international, regional and national level by the countries to counter it. The first section includes the background, including an overview of cybercrime being defined in the various literature. The second section includes various efforts presented on cybercrime legislation including the multilateral instruments such as the convention on cybercrime by Council of Europe, United Nations resolution apart from regional and national efforts. The third section analyzes the challenges of jurisdiction, sovereignty, and privacy and the various responses in the form of legislation being laid out. The fourth section proposes a model for the effective cooperation in the form of balanced multi-stakeholder in light of growing internationalization of the cybercrime.

DOI: 10.4018/978-1-5225-9715-5.ch025

BACKGROUND

2

Literature Review

The research on the cybercrime has focused on analyzing it from various perspective, including the technological, sociological, criminology, psychology, and economic perspective. David Wall (2001, 2007) in one of the early analysis puts cybercrime on the basis of behavior lists (i) Cybertrespass/ hacking (ii) Cyberpiracy (theft of intellectual property) (iii) Cyberpornography (iv) Cyber violence (harassment/ hate speech) as the problem exists on the nature and extent. Later an addition was made to the computer-assisted crime by Susan Brenner (2010) as a social practice with the addition of the cyberspace to all aspects of crime. Due to this addition; cybercrimes are defined on the basis of the “computer enabled” and “computer facilitated” activities. It is similar to the difference earlier categorized by Brenner (2007) of traditional crimes and more specifically defined cyber offenses. The UK investigation agencies make the distinction between the *cyber-dependent crimes* committed through computers directed against computers and other as *cyber-enabled crimes* (Wall 2007). Similarly, (McGuire, 2012) described the cybercriminal groups in the form of “swarms and aggregators” with three types, ranging from the almost virtual conducting illicit activities, hybrid criminal groups and as facilitators mainly traditional organization criminal groups involving in trafficking, gambling, etc.

The definition includes the cybercrime as a form of social practice, which was further articulated by Yar (2013) considers the debates cybercrime not as a single crime but as a broad range of illegal and illicit activities that have effects on societal, political, economic effect. Emilio Viano (2015) in evaluating cybercrime from a societal perspective, considers it as a vastly unregulated field presenting the challenge among policymakers for effective cybercrime regulation. Holt and Bossler et al. (2016) make the distinction that the early computer crime till the 1990s was referred to computer misuse and later with the development of computer and internet, the focus is on offenses in an online environment. What is constructed as an association of crime with cyber is related to the usage of this emerging domain for the traditional criminal activities plus some emerging from the cyber domain. The term “cybercrime” is used to describe a range of offenses, including traditional computer crimes, as well as network crimes (ITU, 2014). Gabriel Weimann (2015) considers the association of terrorism with the cybercrime, where the terrorist has exploited the internet for various means ranging from propagating radical messages to financial gains. Many authors have attempted to look at the extent of the harm caused by the cybercrime empirically which have varied across the reports and limited the real extent in the policy-making (Klahr 2017; Markus Rieke, Rainer Bohme 2018). From a psychological perspective (Kirwan, 2018) in quantifying cybercrimes and propose the effective policing, deterrence means and introduction of a capable guardian to deter the criminal activities. Susan Brenner (2012) identifies the association of the migration of the traditional crime into the cyberspace along with new distinct cybercrime and the need for developing new law for it. Several national laws globally are outdated and face the unique challenge to prosecute them.

Cybercrime Development and Law

The cybercrime originated early on with the spread of networked computers and the legislation for the prevention of it. One of the first legislation was enacted in the US was the *Access device fraud Act* of 1984 for stopping counterfeiting using electronic devices, including computers. The first major cybercrime incident originated in form of Morris Worm which affected computer system in 1988 in the US was

prosecuted under the *Computer Fraud and Abuse Act* passed in 1986 which led to the criminalization of the acts of illegal use of computer. Later sophistication of criminal activities in the cyber domain led to the *Economic Espionage Act* of 1996, making the stealing of the trade secrets and criminal act. New avenues for exploitation because of evolving technology, has brought criminal usage of the computer. The most important change in the cybercrime has been the transition from the early curiosity-driven hackers to financially motivated groups, organized and systematic in the manner (Smith, 2015).

The sophistication of the development of cyberspace has led to challenges for the legislation to deal with the new emerging exploits used by the offenders. The legal approach takes into consideration the efforts for criminalization, (ii) measures for investigation and evidence (iii) harmonization of laws (iv) institutional cooperation, and (v) incident reporting (Appazov, 2014). In defining nature (Brenner, 2010) states the factor affecting cybercrime are proximity, attribution, and lack of physical evidence. Due to the lack of universal definition, the international and regional instrument has been on defining cybercrime on the basis of “set of conduct, making it an umbrella term” (Hakmeh, 2018). Cybercrime is “unbounded crime”; the victim and perpetrator can be in different cities, different states, or different countries. Thereby concealing the identity and making evidence gathering and prosecution difficult.

The recognized base for cybercrime as established in the international documents including Convention on Cybercrime, Tallinn Manual, ITU are:

1. Availability (of the data without any hindrance);
2. Integrity (Authenticity and non-repudiation);
3. Confidentiality (Information for the concerned user only)
4. Computer-related offenses
5. Content-related offenses (includes data theft, password)
6. Copyright –related offenses

The cybercrime legislation refers to policies, laws, recommendations enacted for the prevention and mitigation of computer-related crime. Cybercrime includes traditional forms of crime such as fraud, identity theft, and stalking, bullying, and new emerging forms such as botnets, zero-day exploits, phishing. Cybercrime legislation plays an important role, at both national and international level; in preventing and combating cybercrime. The case for the “formal collaboration” has developed over the years in cyberspace with state-nonstate actors; active state encouragement; state incapacity to control private illegality (Boardhurst, Grabosky, Alazab, & Chon, 2014). ‘Cyberization,’ i.e., in the events such as the 2007 Estonia cyberattacks which rendered critical services ineffective like banking, communications, and government websites reflects the growing offense. The act was being considered under as the potential of having an armed attack. In response, the legislative position of the states has changed over time with the inclusion of the offensive cyberattacks which includes the creation of the cyber military command such as the US Cybercommand and similar efforts by other countries. NATO in 2014 extended the cyber defense in the same category as kinetic attacks. On similar lines, the UN concluded that article 51 referring to the self-defense applied to the cyberspace.

Large scale espionage activities sponsored by the state, such as the large scale Chinese espionage unit revealed by the (Mandiant Report, 2013) reflects a growing association of state and sponsored hackers. The NSA leaks by Edward Snowden exposed a global surveillance program being conducted for the collection of confidential information, including private email and telephone communications (Buchan & Tsagourias, 2016). The consideration of the cyber-related infrastructure as vital in the form of national security have formed an ambit of offensive operations along with the established defensive measures

enacted. The political and economic considerations of cyberspace have changed the definitional aspect of what is accepted and what is not. In the International Strategy for Cyberspace (2011), the United States held for the offense cyber operations defending critical infrastructure at a time when it was facing state-led data breach attacks and economic espionage incidents.

The development of adequate legislation and within this approach, the development of a cybercrime related legal framework is an essential part of a cybersecurity strategy (Brenner, 2010). The integrity of the ICT of a state is essential for the security and economic wellbeing and therefore established national cybersecurity strategies need to reflect it. The steps for the cybercrime legislation includes the criminalization of the acts affecting the integrity, confidently of the computer systems. The early efforts include the OECD in 1983 and the Council of Europe on the criminalization of the offenses in 1989 [recommendation]. Various studies conducted for the crime committed led to studies in 1995 and 1997, which eventually culminated in the Convention on the Cybercrime. The next section discussed the important policies on cybercrime, which includes binding legislation like Convention on Cybercrime and voluntary agreements by the United Nations.

MULTISTAKEHOLDER INSTRUMENTS ON CYBERCRIME

International Approach to Cybercrime

The international efforts for cybercrime consist of international law, development of norms such as the UN GGE (United Nations Group of Governmental Experts), Budapest Convention on Cybercrime, facilitating bilateral agreement and developing deterrence policies in the wake of the development of the attack capabilities. The international agreement consists of the formal and the informal structure and; are voluntary in nature. The broad range of institutions has developed for the construction of facilitating and promoting responsible behavior in cyberspace. This organization operates from the global level to the regional level, ensuring standard operations on the internet and ensuring its security.

The Council of Europe (CoE) Convention on Cybercrime

The convention is the most comprehensive legislation on cybercrime “common criminal policy,” aimed at the protection of the society” at the international level. It was opened for signatories in 2001 at Budapest and remained the only binding instrument in the area of cybercrime (Council of Europe, 2001). The European Committee on Crime Problems established a group in 1996 to form a committee of experts to tackle the issue of cybercrime. The principal rationale for this move was the growing number of cyber-offenses and the need for the updating of the criminal law.¹ Apart from the members of the CoE, there were states including the United States, Australia, South Africa, and Canada in the negotiations process. Through several rounds of meeting and drafts, the Budapest Convention on Cybercrime was opened for signature in November 2001 at Budapest, Hungary to both the members and the nonmembers. The convention entered into force in 2004.

The convention is divided into four chapters covering the criminal acts, laws, enforcement mechanism. The second chapter covers the domestic level procedures for the “criminalization of substantive offenses” (chapter 2-10). An important aspect introduced in the convention related to criminal prosecution was the “collection of evidence in electronic form of a criminal offense.” The significant portions

Table 1. Organizations associated with cyber security and cybercrime

Asia-Pacific economic cooperation(APEC)	International Electrotechnical Commission	Meridian
Association of South East Asian Nations (ASEAN)	International Organization for Standardization	North Atlantic Treaty Organization (NATO)
Council of Europe (CoE)	International Telecommunication Union (ITU)	Organization of American States(OAS)
European Union(EU)	Internet Corporation for Assigned Names and Numbers (ICANN)	Organization for Economic Cooperation and Development
Forum of Incident Response and Security Teams	Internet Engineering Task Force	United Nations
Group of Eight (G8)	Internet Governance Forum	
Institute of Electrical and Electronic Engineers	Interpol	

Source: Key Entities and Efforts with Significant Influence on International Cyberspace Security and Governance [(US GAO, 2010), (Chourci, 2012)]

which cover for the criminalization included: The interference with the data/ System or Illegal Access (ii) Misuse of Devices for crime commitment (iii) Computer-related Forgery and Fraud (iv) Offense related to child pornography. The third chapter laid the international instrument for cooperation, including the mutual legal assistance treaties, transfer of data, and the judicial. For the cross border investigation, the convention facilitates the Laws on the International Cooperation for the purpose of investigation and proceedings. It lays that “the Parties shall afford one another mutual assistance to the widest extent possible” for cooperation on criminal investigation. Also, Article 35 provides for the 24/7 network for the real-time assistance of data information.

In addition, the Council launched the Additional Protocol on Cybercrime on Racism and Xenophobic Nature in 2003 and asserted that the “criminalization of the racist and the xenophobic propaganda committed through the computer systems” and the need for adequate legal responses national and internationally.² The convention forms an integral part on the privacy concerns and the balance of freedom of expression. The council implementing committee T-CY has been regularly updating the convention and negotiation for 2nd Protocol on “enhanced cooperation on cybercrime and electronic evidence” is underway (Council of Europe, 2018). CoE project on Cybercrime includes the harmonization of laws, judicial training, public-private partnership such as the focus on Southeast Europe noted for cybercrime groups and their association with the dark web. The convention is limited to the private actor limiting the scope and does not include action against the states.

United Nations

United Nations (UN) has remained the principle international organization for the development of norms principle and policies in the field of information technology. The role of the UN is to drive the divergences and the harmonization of the laws to reach a common understanding of the laws which can be applicable globally and interoperable with the regional and national laws (Schjolberg & Helie, 2011). The policy-making on the cyber norms at the United Nations consists of two main streams- one politico-military focusing on the cyberwarfare and an economic stream focusing on the cybercrime (Maurer, 2011). The ITU divides the UN organizations ‘work on cyber-security as follows: (1) Combating cybercrime: ITU

and UNODC; (2) Building capacity: ITU, UNIDIR, and UNICRI; (3) Child Online Protection: ITU, UNICEF, UNICRI, UNODC forms the major effort in cybercrime (UN ITU 2010 report). Various bodies, committee's forms part of the policy-making and implementation, including primary bodies the General Assembly and Security Council.

The early legislation on the cybercrime was the UN resolution 55/63 on the *Prevention of Crime* in 1990, which related to the abuse of the computer. The 1998 resolution "Developments in the field of information and telecommunications in the context of security" introduced by Russia in UN General Assembly marked an important shift along with the exponential growth of the internet in the late 1990s (Maurer, 2011). Similarly, the UN resolution *Development in the field of information and telecommunications in the context of international security* (1999); placed emphasis on the development of the principles on international information security and help to combat information terrorism and criminality".³ UN resolution 55/63 and Resolution 56/121 are the main legislation on cybercrime laying framework for the criminalization of computer acts and laying the global legal framework for combating cybercrime (UN, 2001). The main proposition of the legislation is the (i) Eliminate "safe havens" for criminal misuse of information technologies (ii) Coordination of the law enforcement agencies (iii) Criminalization of the acts for violating confidentiality, integrity and the availability of the data. Moreover, the UN Convention on Transnational organized crime (2003) laid a framework for computer usage for criminal activities and the development of training, law enforcement.

A group of governmental experts was formed in 2004 with the aim of strengthening the security of the global information and telecommunication system. (UN, 2003). 2004 agenda was on the "Global culture of the cybersecurity," and the Tunis agenda in 2005 led to two important outcomes; the first was the creation of the Internet Governance Forum (IGF), and second, was the ITU for "Building the Action line C5 for the cybercrime". This action line eventually emerged in the form of the 2007 Global Cybercrime Agenda as a form of the norm-setting agenda on cybercrime under the working of the ITU based on five pillars including Legal Measures; Technical & Procedural Measures; Organization structure; Capacity Building; International Cooperation. The importance of the ITU in UN cybersecurity role is that apart from the organizational role, the agency also acts as an "autonomous norm entrepreneur." The practical guide to *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies* focuses on capacity building of various stakeholders, including education, legal remedies (ITU, 2014). The UN-GGE in recent years has culminated into important consensus on the issue of applicability of international law on cyberspace in 2013 and conduct of state in cyberspace in 2015. Despite the failure to reach consensus in 2017 over the applicability of humanitarian law as the way forward for institutionalizing cyber norms. (Cherneko, Demidov, & Lukyanov, 2018)

REGIONAL LEGISLATION

Apart from the international organization, regional groupings have developed legislation regarding cybercrime in following the harmonization and taking into account the region considerations. The regional legislation has gained prominence as it entails steps for a stronger and detailed legal framework and periodic update of provision with the inclusion of new threat (Dominioni, 2018). This approach is essential as the differences in the region creates a need for a different strategy.

European Union

EU agenda recognizes the cyberspace as a critical area, and the legislation consists of the “larger scope of the EU policies recognizing the international dimension” along with the domestic (Renard, 2018). These are reflected in the “strategic partnerships” as part of the EU cyber diplomacy approach towards a common legal approach; put up in the 2015 cybersecurity strategy. European Union framework on the security of the Information systems, 2005/222/JHA2, and the protection of society (2006) are key directives for the legislation formed. It includes the “stronger national laws” and “severe criminal penalties” (European Union, 2005). The directive changed the institutional response with placing “emphasis rather on approximation” regarding criminal law improving cooperation among authorities and judiciary. (Foggeti, 2009) The directive was replaced by 2013 with the inclusion of new sophisticated attacks as “outlawing of Botnets and ‘using the same point contact as Council of Europe and G8’ for quick action response. (EU 2013)

With the number of cyber threats growing in 2011, the operational measures to combat cybercrime were strengthened. It led to the establishment of EU High Tech crime unit task forces, Cybercrime unit in 2013 with Computer emergency response units and EISAS. The Directive on Security of Network and Information System (NIS Directive) provided a regional wide common legislation on cybersecurity including measures including the illegal interception in the wake of the Snowden revelation apart from illegal data, system interference (Munroe 2017). It includes the formation of National CIST, data sharing collaboration, and harmonization of laws.

EU internal strategy was adopted in 2010 with the future layout for directives containing protection of the data and fundamental rights in the directive enacted. The European Union General Data Protection Regulation (GDPR) enforced in 2018 has changed the ways of privacy and security with “data as a fundamental right” at the individual level. This affects the way data is collected, processed and stored, where ‘consent’ is required for any form of data collected and to be reported to a competent national supervisory authority in case of violation (European Union, 2016). For cybercrime, the data handled is segregated by the authorities and the liability of the companies handling the data with fines up to 4% of the global turnover. These are important steps at times when data breach and the ransomware incidents have sharply grown. The legislation debate has a worldwide effect on the concern for privacy being placed along with security measures at the national level.

Other regional organization proceeds on the basis of voluntary agreement, Shanghai Cooperation Organization⁴ Agreement on Cooperation in the Field of International Information Security (2009) defines the “key concepts and main threats” to the information security. The agreement differs from other western conventions referring to the protection of the information security, including the socio-political, economic, cultural, and moral environment of the state” (SCO, 2009). The SCO legislation was adopted at UN ‘Code of Conduct for Information Security’ in 2015 which contains measures for the protection of information security [defined in a broad manner] with focus on the national sovereignty and data localization efforts to combat cybercrime.

The League of Arab States Convention on *Combating Information Technology Offences* (2010) the convention has drawn from the Budapest Convention in the provisions. (Hakmeh, 2018). However, the religious factors are included, which is unique such as “ideas and principle of terrorist groups.” The focus has been on the criminalization of acts and limitation of freedom of expression with vaguely wordings. (Hakmeh, 2018)

ASEAN, the organization of Southeast Asian states declaration to prevent and combat cybercrime was adopted in 2007, emphasize the “importance of harmonization of laws related to cybercrime and electronic evidence.” ASEAN Cyber Capacity Development (2016-2020) is part of the ongoing process to develop comprehensive region-wide legislation, enforcement with a comprehensive review of national laws and developing capacities (AT Kearney, 2018). The efforts become important as cybercrime are transnational in nature with the region witnessing massive IT growth.

African Union Convention on Cybersecurity and Personal Data Protection (2014) recognizes cybercrime as a “real threat to the information society in African Union” defined broad guideline to combat cybercrime and protection of personal data (African Union, 2014). It calls for the formation for national cyber strategy by each member state to combat cybercrime (Article 24) and the formation of National Data Protection authorities (Article 11). Similarly, other nonbinding efforts by regional organizations include the Association of Pacific Economic Community (APEC) which has security and prosperity steering group overseeing the efforts for the prevention of cybercrime. Similarly, the Organization of American States (OAS) has a dedicated Inter-American Cooperation Portal on the resources and data relating to cybercrime.

NATIONAL CYBERCRIME LEGISLATION

Various states have adopted the measures for the protection in the form of legislation enacted paving the way for the criminalization of the acts. The current position is that cybercrime legislation is as of now enacted by 135 countries out of which 95 are developing⁵, and still, more than 30 countries have not enacted any cybercrime legislation (UNCTAD 2018). The developed states still lead for international harmonization of the cyber laws, and several states follow the Convention on Cybercrime, which guides the member and the non-member states. National legislation contains measures to ensure the availability, integrity, and confidentiality of data and protection of the critical information systems. To keep pace with technology development, many countries use “generic language to generalizations” in cybercrime legislation reflected in the United Kingdom and US legislation.

In the U.S, the *Computer Abuse and Fraud Act 1987* are being used to criminalize the acts of illegal and illicit use of the computer along with the setting of computer emergency response network (CERT) (Viano, 2017). The issue of copyright infringement, intellectual property, and identity theft have been covered by various federal Act such as the 1998 *Identify Theft and Assumption Deterrence Act*. The increase of the ransomware as a significant cybercrime issue has led to the enactment *Economic Espionage Enhancement Act* of 2012 and safeguards for Intellectual property theft. In 2015, executive order 13964 was enacted by the Obama administration with the application of economic sanctions to hackers.

In the UK, the *Computer Misuse Act* of 1990 forms the base of criminalization of illegal access to the computer. However, significant addition has been added to such as computer misuse act in the UK in 2015, putting cybercrime to serious crime with increased imprisonment to 14 years. On the other hand, Australia government produced legislation titled the *Cybercrime Amendment Act of 2012* to implement all the clauses of the Convention on Cybercrime to strengthen cybercrime laws. The primary provision includes stronger communication measures “held by the carriers” required under warrant for investigation (Australian Government, 2012).

The Chinese cybercrime law introduced in the Penal Law of 1997 makes illegal access to the computer punishable and also includes the damage to the hardware of the computers. The 9th amendment to the Penal Law was placed in 2014 with penalizing network operators to failure of obligations and provide support, information to criminals. In the comparative paper by (Yong, 2011) between Chinese cybercrime laws and Convention on Cybercrime describes that the parties which have not signed the convention have used it as a reference point for legislation formulation.

Also, India, which is not a signatory to the Council of Europe, has modeled its cybercrime law on the United Nations resolution according to the harmonization of national legislation. Information Technology Act, 2000 forms the base for legal recognition to all electronic activities and making the criminalizing act of illegal access to a computer. Amendment to the law in 2008 have included liability of the companies for the data breach, e-commerce transactions, child exploitation online. The cybersecurity law of 2013 furthers the growing importance on infrastructure with specialized agencies and cooperation on the cybersecurity issues.

Apart from multilateral cooperation, bilateral cooperation between states serves as a *direct point of contact* resolving the disputes and enabling cooperation. Currently, the various bilateral agreement extends on several areas, including cybersecurity, data transfer, and law enforcement between countries. The U.S.- China agreement (2015) on the cyber-enabled economic espionage or the US-India cybersecurity agreement (2013) aims to strengthen security and cooperation. Similarly, Russia- China agreed on the ‘non-aggression’ garment with the aim to not attack each other ICT enabled systems.

SCOPE OF CYBERCRIME LEGISLATION: CHALLENGES

The cybercrime legislation has a considerable difference from the legislation on traditional crime with respect to the location of the criminal due to the issue of attribution. The physical presence is not necessary in the case of cyberattacks, as most of the crime is committed transnationally placing the difficulty of jurisdiction. As the legislation encompasses information security, the onus of securing privacy is difficult to reach. In the Convention on Cybercrime, article 32 (B) refers to the “transborder access to data where publicly available.” The interpretation has been dubbed as an overreach of the data leading states like Russia not signing the convention.

Jurisdiction

The applicability of the criminal laws in the international sphere takes place in the form of procedural law and substantive law. The principle of “Dual Criminality” places that the offender can be prosecuted irrespective of the place the crime was committed if the same set of laws exist in both the countries. Tallinn Manual 2.0 places the question of the extraterritoriality ‘from a new position. The “meant to be accessible” (rule 8 of the manual) is the determining factor that, if the counties access the public data from their territory [though located overseas] is not an act of extraterritoriality but the case of territoriality (Eichensehr, 2017). In adjudicating the case of the Microsoft v. the United States on the accession of the data located on a server in Ireland, Second Circuit court ruled in favor of Microsoft considering it overarching of the Stored Communication Act (SCA). However, the U.S Supreme Court overturned the

case as “unauthorized extraterritorial application” in favor of Microsoft. (*United v. Microsoft Corps.*, 2018). In the debate Cloud Act⁷ passed by the U.S Government amended the SCA and placed the capabilities to access overseas data [if it does not violate the law of the country] and access the data in the U.S [not targeting U.S citizens or person within the United States](Cloud Act 2018). Further, it allows the President to enter into an executive agreement for data transfers with other countries. The question of global enforcement found relevance in the massive ransomware attacks as Petya Malware, which was a series of Denial of Service attacks (DDoS) and affected computers in over 150 countries.

Sovereignty

The cyberspace has emerged as a new avenue for competition among various actors. State-sponsored cybercrime has increased over the years, where the states are allegedly committing cybercrime in the form of digital espionage, surveillance, and network interference activities. The problem of attribution, i.e., “who committed” has occurred with debates over digital evidence in prosecution. UN-GGE concluded that international law applies to cyberspace, state sovereignty, and the resulting laws; asserting the state rights in the domain. The actions are limited with the question of attribution and the prosecution of cybercriminals as in the case of Estonia cyberattacks in 2007 sponsored by Russia.

Rule 8 of the CoE holds the fact that a cyber-operation has been routed via the cyberinfrastructure located in a state is not sufficient evidence for attributing the operation to that State. The Group of 7 (G7) declaration on “Responsible States Behavior in Cyberspace” recognized on April 11, 2017 underlines that “the urgent necessity of increased international cooperation to promote security and stability in cyberspace consisting of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime” and reaffirmed “that the same rights that people have offline must also be protected online.”

Data Transfer and Privacy Concerns

Privacy has remained important and grown more central to the cybercrime legislation. The number of data breaches has escalated over the years. The need to identify and legislate to apply changes in this domain has become central to the recurring debates in the socio-political domains, triggered by daily cyber-related incidents. The legislation, in many ways, provides means to law enforcement agencies to store more data. At the same time, incidents of data breaching of identity theft, financial information has increased. The collection of the metadata under the Patriot Act and the Edward Snowden revelation has led to the increased concerns for the protection of data. Social networking websites such as Facebook has witnessed massive data breaches. The EU data retention directive of 2006 was annulled in 2014 by Ireland Court on the basis of fundamental rights to respect for private life and to the protection of personal data” (Digital Rights Ireland and Seitlinger, 2014). The set of factors are reflected in the emergence of the data localization by states including Russia, India, and China has emerged with the storage of user data within the territory and control of the major companies. EU privacy policy places the “adequacy protection” in personal data with the power to determine the country has “adequate level of data protection.”

RESPONSE

Legislative Position on Investigation and Enforcement

The case of global internet governance is as much a political as it is technical (Shull 2014). The European Council Guidelines for Internet Service Providers and Law Enforcement Cooperation, especially in the prevention, investigation, and data evidence cases⁸. The various mechanisms developed in the form of the formal and informal cooperation result as “requisite consensus,” which is still being developed (Munroe, 2017). Data forms the vital part of the information technology, and the effective legislation on the sharing of the data remains to be “complex and sensitive” with the information exchange diverse the trust deficit among the states (Rutkouski, Fostr, and Goodman, 2012). The actions driving the work of the international law enforcement bodies are in the position of advisory function. G7 cybercrime working group (Roma-Lyon Groups High Tech Crime Subgroup) developed 24/7 point of contact for “requesting on an emergency basis preserving electronic evidence and locate suspects” (OAS). It is especially important for the foreign government to request for electronic evidence to major ISP and extends to include 84 states⁹ as members.

Interpol, the major international investigation agency, consists of 190 states tends to aid the investigation agencies in various states. In the form of the capacity building initiatives, they prepare the law enforcement officials and monitoring of the “norms and instruments” connected to the cybercrime (Interpol, 2017). In 2010, the Global Complex for Innovation (GCI) was formed by its general assembly and later including the Digital Crime Center with the mandate of “global hub for cybercrime issues” (Schjolberg, *The History of Cybercrime: 1976-2014*, 2014) Partnering with the private players, remains vital in fight against the cybercrime. Interpol Global Complex for Innovation signed the data sharing agreement with British Telecom for “threat information exchange on data relating to criminal trends in cyberspace” (BT (British Telecom), 2017).

Global Multilateral Alliance¹⁰ as IMPACT formed in 2008 backed by the United Nations represents the partnering between the government and the private industry. The alliance has now 152 members with the services including emergency response service, identification of the cyber threats and sharing resources across the member states. The action is important for the states developing the national emergency response system for cyber threats (IMPACT, 2012). In the form of the institutional response, Europol the primary law enforcement agency in European Union, set up the European Cybercrime Center (EC3) to drive action through “cross- border investigation” and operations by partners with the private players.

There is a well-established informal process which supports the formal process (Smith, 2015). The other informal efforts apart from IMPACT include Meridian process which handles the regularly updated global reference book for Critical Information Infrastructure Protection policies and points of contacts for technical cyber emergencies in more than 50 countries. Besides this, the Global Cybersecurity Index launched in 2014 helps foster a global culture of cybersecurity and its integration at the core of ICTs (ITU, 2017). A financial Action Taskforce (FATF), an intergovernmental body formed by the European Council with the rationale of protecting the global financial system in 2014 published report on Virtual Currencies. The FATF group comprised of states including the United States and Russia laying out the key definition and developed a “risk matrix” for bringing clarity and understanding financial risk from cybercrime. The step is imperative as the ransomware industry has grown with the usage of new sophisticated tools such as Eternal Blue the tool used by NSA was leaked and used for Petya malware attacks.

At the national level concerns over the applicability of domestic law to international crime, situations sustain. In the case of the United States, the case of extraterritoriality applies with the provision of the Patriot Act and now Cloud Act allows for the “search and seizure of the data” publicly available. The measures and the issues in international law with the lengthy procedure involved the formalized channel for the collection of the electronic evidence is essential to bring cybercriminal indictment. This is especially important between states that are not a member of grouping like Convention on Cybercrime, e.g., China, India. The position is quite similar to the discussion by the UNGGE experts of the “publicly” available data in foreign territory.

For serving as the model legislation in cybersecurity, the EU e-evidence directive for improving the cross border investigation and the preservation of electronic evidence for criminal purposes, EU e Directive extends the service provider obligation with direct evidence production from one member state to other. The act is still under consideration with the criticism for the over compliance and the necessary safeguard for data. Also, way forward has emerged in policies of the European Union with the creation of a *single digital market* and EU wide cybersecurity strategy in the form of binding implementation. The Network and Information Directive (NIS) directive puts EU states to identify the strategic resources, common cooperation groups for sharing strategic information

The legislation for conducting the state behavior has also gained momentum with the UN GGE call for responsible state behavior, while private organization Microsoft called for a ‘Digital Geneva convention’ regulating state behavior in state-led attacks.

Cybercrime Regulation Proposed Approach- A Balanced Multistakeholder Model

Maurer (2011) contends that Internet governance has traditionally not been dominated by states but rather by the private sector and civil society. The increasing number of internet users have escalated the people affected by cyber legislation. This is the ——multilateral (states only) vs. ——multi-stakeholder (states plus private sector and civil society) debates, reflecting the position on the issue. Western countries have pushed for Convention on Cybercrime, while states such as Russia, China on alternate models of internet governance focuses on sovereignty. An important aspect is the reform of the internet governance stricter within which the domain name, registry, and the working of the internet lie. China, along with other developing states, demanded the reform of the ICANN, which distributes the domain name system on which the internet works. The current structure is dubbed as “legitimacy crisis,” especially the working of the structure as ICANN governing bodies. The events are more incited due to the activities of the events such as Edward Snowden leaks exposing large surveillance programs and the cyber legislation, the international consensus due to the working model of the internet governance where the western countries dominate the structure and legislation. The larger role of the ITU in the role in the building initiatives in the development of the national strategies, legislation, enforcement, and organization structures fulfill the digital divide. (ITU, 2012)

The proposed model views the process as balanced, equative, and collaborative of all the relevant partners, especially in the harmonization of legislation, sharing of data and effective law enforcement. Particularly, the model holds importance when the cybercrime in the developing countries has seen surge; with the states having “few or no laws against cybercrime.” (Kshetri, 2010)

Therefore, the capacity building initiatives in the development of national strategies, legislation, enforcement organizational structures is desperately needed (ITU, 2012). The formal structure is one way while collaboration is another, which includes the informal process, i.e., the inclusion of partners and mechanism along with government and its associated institutions. The UNODC report of 2013 emphasizes the primacy of capacity building for at all the levels of the individuals, governments, enforcement agencies. (UNODC, 2013). Human error in the cybercrime perspective constitutes 27 percent of the security lapses forming substantial loss (IBM, 2018). Therefore, the provisions for educating the users regarding the various protection mechanisms should be placed. The confidence building exercises are an effective way of further leveraging the relations. EU dialog with China in the form of 1.5 track Sino-European cyber dialog or U.S-China cybersecurity dialog reflects the developing effectiveness of cooperation on cybercrime issues. The Global Cybersecurity Index report 2017 concluded that “the collaboration of the developed countries in training of the local cybersecurity experts and more cooperation to assist them in cybersecurity development,” thus emphasizing the necessity for multi-stakeholder efforts. (GCI 2017)

CONCLUSION

The conversation of digital activities into crimes related to cyber technology has emerged as the base for the cybercrime policies at the international, regional, and national levels. Convention on Cybercrime is an effort towards harmonization of laws at the international level. Yet, it remains the only binding instrument at the international level, reflecting the urgency to resolve issues that need to be addressed. The growing prominence of organized crime and state-sponsored groups has furthered the need for global cybercrime regulation. The UN nonbinding voluntary basis mechanism has worked towards the institutionalizing and garnering consensus among states for developing and implementing cyber laws, though on a limited scale. EU GDPR presents the way forward, strengthening the data collection mechanism and entrusting privacy safeguards, especially in the wake of data exploitation by numerous actors for malicious purposes. The proposed balanced multistakeholder model can be an effective mechanism for bringing comprehensive international efforts to combat cybercrime. With an emphasis on developing countries, which include a vast amount of internet infrastructure and users, their role becomes prominent in the governance of the internet and policymaking.

REFERENCES

- Accenture. (2017). *Cost of Cybercrime Study*. Ponemon Institute. Retrieved November 2, 2018, from https://www.accenture.com/t20170926T072837Z__w_/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
- African Union. (2014). *African Union Convention on Cybersecurity and Personal Data Protection*. Author.
- Appazov, A. (2014). *Legal Aspects of Cybersecurity*. Copenhagen: Justitministeriet Denmark. Retrieved January 11, 2019, from http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

Australian Government. (2012, September 12). *Cybercrime Legislation Act120(2012). An Act to implement the Council of Europe Convention on Cybercrime, and for other purposes*. Retrieved October 30, 2018, from <https://www.legislation.gov.au/Details/C2012A00120>

Boardhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8(1), 1–20. Retrieved from <http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf>

Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, CA: Praeger.

BT (British Telecom). (2017, Oct 17). *BT and Interpol Unite to Fight Cybercrime*. Retrieved from BT: <https://www.globalservices.bt.com/en/aboutus/news-press/bt-and-interpol-unite-to-fight-cybercrime>

Buchan, R., & Tsagourias, N. (2016). Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence. *Journal of Conflict and Security Law*, 377-381. doi:10.1093/jcsl/krw017

Cherneko, E., Demidov, O., & Lukyanov, F. (2018). *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*. Council on Foreign Relations. Retrieved December 2, 2018, from <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms>

Chourci, N. (2012). *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press.

Council of Europe. (2018, March 19). *T-CY Drafting Group*. Retrieved from Council of Europe: <https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713>

Digital Rights Ireland and Seitlinger. C-293/12 and C-594/12 (Court of Justice of the European Union April 8, 2014). Retrieved September 29, 2018, from <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

Dominioni, S. (2018, July 16). *Multilateral tracks to tackling cybercrime: an overview*. Retrieved November 5, 2018, from Italian Institute for International Political Studies: <https://www.ispionline.it/en/pubblicazione/multilateral-tracks-tackling-cybercrime-overview-20962>

Eichensehr, K. E. (2017). Data Extraterritoriality. *Texas Law Review*, 95, 145–160.

European Union. (2005, February 24). *Council Framework Decision 2005/222/JHA*. Retrieved from EUR-LEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN>

European Union. (2016, May 4). *(EU) 2016/679. The protection of natural persons with regard to the processing of personal data and on the free movement of such data*. Retrieved November 25, 2018, from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

FATF. (2014). *Virtual Currencies: Key Definitions and potential AML/CFT Risks*. Geneva: Geneva Internet Platform. Retrieved from www.fatf-gafi.org

Foggeti, N. (2009). *Transnational Cybercrime Differences between national laws and development of European Legislation: By Repression?* Academic Press.

Hakmeh, J. (2018). *Cybercrime Legislation in the GCC Countries: Fit for a Purpose?* International Security Department. London: Chatham House. Retrieved November 11, 2018, from <https://www.chatham-house.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf>

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. New York: Routledge Press.

IBM. (2018). *2018 Cost of a Data Breach Report: Global Overview*. Ponemon Institute.

IMPACT. (2012). *IMPACT: International MULTilateral Partnership Against Cyberthreats*. Retrieved November 22, 2018, from ITU: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

Interpol. (2017, March). *Collective Action Against Cybercrime*. Retrieved November 21, 2018, from <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKEwjshOjXtfHeAhVIqI8KHdedBf8QFjAlegQIARAC&url=https%3A%2F%2Fwww.interpol.int%2FMedia%2FFiles%2FAbout-INTERPOL%2FIGCI%2FInformation-Sheets%2FCollective-action-against-cybercrime%2F&usg>

ITU. (2012). *Understanding cybercrime: Phenomena, challenges and responses*. Geneva: International Telecommunication Union. Retrieved November 29, 2018, from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

ITU. (2014). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva: International Telecommunication Union. Retrieved December 1, 2018, from <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx>

ITU. (2017). *Global Cybersecurity Index (GCI) 2017*. Geneva: International Telecommunication Union.

Kearney, A. T. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action*. Singapore: Academic Press.

Kiggins, R. D. (2014). US Leadership in Cyberspace: Transnational Cybersecurity and Global Governance. In J. F. Kremer & B. Muller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 161–180). Heidelberg, Germany: Springer Press. doi:10.1007/978-3-642-37481-4_10

Kirwan, G. (2018). The Rise of Cybercrime. In C. F. Alison Attrill-Smith (Ed.), *The Oxford Handbook of Cyberpsychology*. Oxford Handbooks Online. doi:10.1093/oxfordhb/9780198812746.013.32

Maurer, T. (2011). *Cybernorm Emergence at the United Nations: An analysis of the activities at the UN regarding cybersecurity*. Belfer Center for Science and International Affairs. Cambridge, MA: Harvard Kennedy School.

McGuire. (2012). *Organized Crime in the Digital Age*. London: John Grieve Center for Policing and Security.

Nye, J. (2011). *The Future of Power in the 21st Century*. Cambridge.

OAS. (n.d.). *The G8 24/7 Network of Point Contacts*. Retrieved from *Organization of American States*.

Radu, R. (2014). Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In J. F. Kremer & B. Muller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 3–20). Heidelberg, Germany: Springer Press. doi:10.1007/978-3-642-37481-4_1

Renard, T. (2018). EU Cyber partnerships: assesing the EU strategic partnerships with thid countries in the cyber domain. *European Politics and Society*, 1-19.

Report, M. (2013). *APT1: Exposing One of China's Cyber Espionage Units*. Retrieved November 11, 2018, from <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

Rieke, M., & Bohme, R. (2018). The costs of consumer-facing cybercrime:an empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*. doi:10.1093/cybsec/tyy004

Schjolberg, S. (2014). *The History of Cybercrime: 1976-2014*. Norderstedt: Herstellung und Verlag.

Schjolberg, S., & Helie, S. G. (2011). *A Global Treaty on Cybercrime and Cybersecurity*. Oslo: AiTOslo.

SCO. (2009). *SCO Documents*. Retrieved from Shanghai Corporation Organization: <http://eng.sectsc.org/documents/>

Shea, J. (2017). How is NATO meeting the challenge of Cyberspace? *Prism*, 19–29. Retrieved from https://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/3-How_is_NATO_Meeting_Challenge_of_Cyberspace.pdf?ver=2017-12-21-110643-000

Smith, R. G. (2015). Trajectories of a Cybercrime. In R. Smith, R. Cheung, & L. Lau (Eds.), *Cybercrime Risk and Responses: Eastern and Western Perspectives*. London: Palgrave Macmillan. doi:10.1057/9781137474162_2

The White House. (2011). *International Strategy for Cyberspace*. United States Government Printing Office. Retrieved November 13, 2018, from https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

UN. (2001, January 22). *UN General Assembly*. Retrieved from A/Res/55/63: Http: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

UN. (2003, December 18). *UN General Assembly Resolution*. Retrieved from A/Res/ 58/32.

UN GGE. (2013, June 24). *Development in the Field of Information and Telecommunications in the context of international Security*. New York: United Nations Publications.

United v. Microsoft Corps., 584, U.S. (2018). Retrieved October 28, 2018, from <https://supreme.justia.com/cases/federal/us/584/17-2/case.pdf>

UNODC. (2013). *Comprehensive Study on Cybercrime*. Vienna: United Nations.

US GAO. (2010). *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*. United States Government Accountability Office. Retrieved November 2, 2018, from <https://www.gao.gov/new.items/d10606.pdf>

Viano, E. C. (2017). Cybercrime: Defination, Typology and Criminalization. In E. C. Viano (Ed.), *Cybercrime, Organized Crime and Societal Response*. Washington, DC: Springer Press. doi:10.1007/978-3-319-44501-4_1

Wall, D. (2001). *Crimes and the Internet: Cybercrimes and Cyberfears*. London: Routledge Press. doi:10.4324/9780203164501

Wall, D. (2007). *Cybercrime: the Transformation of Crime in the Information Age*. Academic Press.

Yar, M. (2013). *Cybercrime and Society* (2nd ed.). Sage Publications.

Yong, P. (2011). *New China Criminal Legislations in the Progress of Harmonization New China Criminal Legislations in the Progress of Harmonization*. Retrieved November 29, 2018, from <https://rm.coe.int/16803042f0>

KEY TERMS AND DEFINITIONS

Cloud Act: Cloud Act is the U.S. legislation related to the transfer of electronic data with provisions for obtaining data for evidence and prosecution and also regulating transfer for foreign governments.

Cybercrime: The usage of the computer and its related technologies for the purpose of disrupting, with the motivation to gain financial gains or causing political, social, and psychological harm.

Dark Web: The dark web is part of the web that is not accessible on general search and can be accessed through specific hosting servers. It consist of the information and tools that are illegal by criminal, terrorist.

Denial of Service Attack (DDoS): The activities which disrupt the services of the computer rendering the computer usage ineffective for the user.

Mutual Legal Assistance (MLAT): MLAT are formal investigation request made by the states for the access of the data located in other country for the purpose of investigation and extradition.

Phishing: Is defined as the method of cyberattack which are employed to capture the sensitive information including passwords, personal information for the malicious purpose through means such as deceptive emails.

Ransomware: Is defined as the illegal access to computer system using malware for the purpose of gaining control of the system with the motivation for financial gains.

ENDNOTES

¹ See the explanatory note to the Convention on Cybercrime for other rationale including academics works, Available at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

² See, European Treaty Series NO. 189, Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer system, January 28, 2003.

³ UN General assembly A/RES/53/70, 4 January 1999.

⁴ SCO consists of seven member states including China, Russia, Tajikistan, Kazakhstan, and Turkmenistan and now also includes India and Pakistan.

- ⁵ The database of the national legislation of all the states is available at Repository of Cybercrime at United Nations Office on Drugs and Crime, 2018, <https://sherloc.unodc.org/cld/v3/cybrepo/legdb/index.html?lng=en>
- ⁶ Where one country asserts jurisdiction over persons or events outside its borders, this is regarded as “extra-territorial” in its reach. (pg. 202 Russell Smith)
- ⁷ Clarifying Lawful Overseas Use of Data (2018) is the U.S law (115-141) for the collection and processing of data with other countries and the private companies.
- ⁸ The guidelines are within the working of the Council of Europe Convention 2001 law.
- ⁹ The latest state to join is Tonga, see the link http://www.mic.gov.to/index.php?option=com_content&view=article&id=7436&lang=es
- ¹⁰ For Full list of the alliance members, industry partners including key initiatives, see the policy document paper 2012, available at: <https://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf>

Regulating the Internet

David T. A. Wesley

Northeastern University, USA

INTRODUCTION

The early history of the Internet was a time of naive optimism that the medium would create a new era of global free speech. In 1996, John Barlow, an Internet Pioneer and founder of the digital rights organization known as the Electronic Frontier Foundation (EFF), wrote “A Declaration of the Independence of Cyberspace” in which he declared that governments “have no sovereignty” over the Internet. Cyberspace was “naturally independent of the tyrannies” of nation states, he wrote, and any attempts to control it would ultimately fail (Barlow, 1996).

More than 20 years later, Google is creating a search engine for China that censors any content deemed disagreeable to the central government, Facebook is being used by hate groups to organize lynch mobs and commit genocide, and Internet-connected cameras are being deployed for mass surveillance. The Internet has also become a primary tool for state propaganda and “fake news” aimed at undermining democracy and free speech.

Despite these challenges, court decisions that protect computer code under the First Amendment of the United States constitution have helped create a free flow of knowledge and tools that can be used to counter such threats. Given the ubiquity of American technology companies, U.S. legal precedents and decisions can have global implications.

FOCUS OF THE ARTICLE

Established U.S. law has long held that computer code is a language, like any other language, and is therefore subject to same free speech protections afforded other forms of speech under the First Amendment of the United States Constitution. Computer code also protects free speech through cryptography that enables protected communication between two or more parties.

This article will consider the legal history of computer code as free speech and how it can be used to promote other forms of free speech through cryptography and secure communications. It will further argue that the deep web and dark web are direct results of these precedents and while they can be abused by cybercriminals and malicious state actors, they are also indispensable in promoting free speech and human rights.

BACKGROUND

The telegraph was one of the first uses of technology to communicate information. In the early 20th century, the language of automatic telegraph operators in many ways resembled computer code. For example, when a telegraph operator would send a message, the message was encoded with special

DOI: 10.4018/978-1-5225-9715-5.ch026

terms – dux for duplex, mux for multiplex, gm for good morning, etc. With the advent of the automatic telegraph, words such as printers, machines, and bugs took on new meaning. A bug, for example, was an electrical disturbance that could cause the signal to drop out momentarily or even cause the system to hang (Brackbill, 1929).

Similarly, the first computer engineers created unique computer codes that later developed into their own languages. In the 1950s, as computers became more complex, engineers began to recognize the problem of making this increasingly complex machine language intelligible. Brownson (1953) wrote, “In communicating with each other, we seek to communicate concepts; in defining terms for manipulation by computers, man will have to find out exactly what he believes and make coherent and integrated sense of it.”

Bar-Hillel (1953), a pioneer in machine translation, saw this as “a real challenge for structural linguists,” but he also believed that it would only be a matter of time before machines acquired a “semantic organ.” “One of the decisive steps in certain methods of machine translation is the determination of the syntactic structure of any given sentence in the source-language (i.e., the language from which we translate) to a required degree of explicitness.” As a result, computers that “were originally designed to solve certain mathematical problems... might well be recombined to yield similar results in noncomputational fields” (Bar-Hillel & Bar-Hillel, 1951).

Already, Brownson and Bar-Hillel were expressing two views that would later become central in the debate over computer code as free speech. Brownson saw computer code as a form of communicating what one believes, whereas Bar-Hillel saw it as a means to solve problems, including those that were strictly mathematical and those that would later develop in noncomputational fields. If computer code expresses ideas and beliefs, it could be a protected form of speech under the First Amendment to the United States Constitution, but if, as Bar-Hillel says, it is merely a method to solve problems, then it should not be protected.

Two of the earliest cases to consider the question of the First Amendment status of computer code involved export restrictions on cryptography programs. In 1996, President Clinton issued an executive order restricting the exportation of encryption products in the interests of national security. Henceforth, encryption technology would be “designated as defense articles in Category XIII of the United States Munitions List and regulated by the United States Department of State pursuant to the Arms Export Control Act” (Executive Order 13026, 61 Fed. Reg. 58767).

In *Karn v. United States Department of State* (1996), the court made “no ruling as to whether source codes... fall within the protection of the First Amendment,” but clearly suggested that it was not protected when it stated that “[s]ource codes are merely a means of commanding a computer to perform a function.” In this case, the court applied the O’Brien test (*United States v. O’Brien*, 1968), holding that the “government regulation at issue here is clearly content-neutral” and that the government had a compelling national security interest at stake.

This contrasts the position in *Bernstein v. United States Department of State* (1996), in which the Honorable Marilyn Patel held that “the particular language one chooses [does not] change the nature of language for First Amendment purposes. This court can find no meaningful difference between computer language, particularly high-level languages as defined above, and German or French. All participate in a complex system of understood meanings within specific communities. Even object code, which directly instructs the computer, operates as a ‘language.’ When the source code is converted into the object code ‘language,’ the object program still contains the text of the source program. The expression of ideas, commands, objectives and other contents of the source program are merely translated into machine-

readable code.” The different views of the Karn and Bernstein courts reflect the same questions raised by linguists like Brownson and Bar-Hillel, namely is computer code expressive or functional.

Both Karn and Bernstein were faculty members at U.S. universities who used encryption examples to teach computer science students about programming. Karn was permitted to export his textbook, but he was prohibited from exporting a floppy disc that contained a verbatim copy of the book. The only difference was that one was digital and the other was on paper (Camp & Lewis, 2001). However, in *Reno v. ACLU* (1997), the Supreme Court held that discrimination by media type was unconstitutional. An opinion delivered by Justice Stevens found that no distinction existed because of the medium used to communicate ideas. In reference to the Internet, which like a floppy disc is digital, he stated “that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.” He also referred to the district court’s opinion that the Internet is “the most participatory form of mass speech yet developed” and is therefore “entitled to ‘the highest protection from governmental intrusion.’”

Around this time, the rapid growth of the Internet led most academic publishers to stop issuing computer discs with textbooks. Instead, they posted examples on websites. However, because of the global nature of the Internet, the posting of encryption code on websites fell under the same export ban on encryption code as computer discs. In *Junger v. Daley* (2000), a university professor challenged a government ruling that he was not allowed to post encryption code on his website, even though his textbook containing the same code could be exported. In that case, the court held that computer code was protected by the First Amendment “[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming.” The court also found that even if the code is primarily functional in nature, it is still protected by the First Amendment under *Roth v. United States* (1957), in which the Supreme Court stated that “ ‘all ideas having even the slightest redeeming social importance,’ including those concerning ‘the advancement of truth, science, morality, and arts’ have the full protection of the First Amendment.”

Another issue that was not addressed in the aforementioned cases is the role of encryption code in promoting the constitutionally protected free speech of others. Many countries suppress free speech as a way to control their citizens, to maintain state secrets, and to cover up human rights abuses. Organizations like Amnesty International rely on “encryption to protect their files and communications from seizure and interception by the governments they monitor for abuses” (Madsen, Sobel, Rotenberg, & Banisar, 1997).

The ability to disseminate and discuss cryptographic code has important value in protecting the First Amendment rights of American human rights workers who are living abroad. In *Broadrick v. Oklahoma* (1973), the U.S. Supreme Court held that litigants “are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute’s very existence may cause others not before the court to refrain from constitutionally protected speech or expression.”

The fact that these human rights organizations are operating in other countries does not diminish the First Amendment rights of the plaintiffs, who were U.S. citizens developing and disseminating code from within the United States. In *Yahoo!, Inc. v. La Ligue Contre Le Racisme* (2001), a U.S. company was convicted in a French court for disseminating information in France that violated French law, namely Nazi memorabilia. However, because the publication originated in the U.S., the U.S. District Court for the Northern District of California held that while “first amendment protections do not apply to all extraterritorial publications,” protections for “actions in the United States” do apply.

The development of “dark web” tools, like the Onion Router and the TOR browser, was funded by the U.S. Naval Research Laboratory in partnership with the Free Haven Project, “to promote unfettered

access to the internet in locations where online censorship was heavily enforced or where the threat of persecution for those who sought access to locally illegal information was prohibitive” (Moore and Rid, 2016). Although often vilified in movies like *Unfriended* and *Nerve*, TOR’s developers continue to focus on protecting journalists and human rights activists (Zetter, 2017). Not only do these dark net tools continue to play an important role in global free speech, they also enjoy the same legal protections.

Having established that computer code is speech deserving of First Amendment protection, the next question is whether the government has a compelling interest to regulate that speech. Clearly, cryptography can play an important role in national security concerns, such as drug trafficking and terrorism (Ferrera, 2004), but in cases where the courts have decided for the plaintiffs, the artistic and educational value of computer code outweighed this state interest. Cryptography also has important commercial value protecting trade secrets, banking records, and digital content, such as games, music, and movies. More importantly, it has a social value in protecting the free speech and free association of individuals and organizations, preserving the human rights and dignity of vulnerable populations, and preserving a free press.

SOLUTIONS AND RECOMMENDATIONS

American security is better served with unbreakable end-to-end encryption than it would be served with one or another front door, backdoor, side door, however you want to describe it. - Former CIA Director, General Michael Hayden (2016)

Arquilla and Ronfeld (1993) of the U.S. Naval Postgraduate School long predicted that “widespread multi-organizational networks that have no particular national identity” would attempt to undermine civil society. “A netwar may focus on public or elite opinion, or both,” they explained. “It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.”

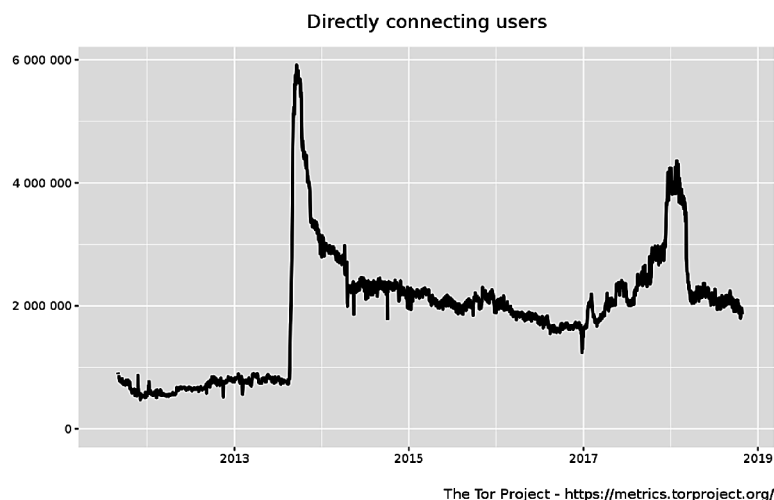
Twenty-five years later, social media is being used to promote authoritarianism, populism, and nationalism. Facebook and WhatsApp have become the de facto tools used by hate groups to encourage genocide in Africa, India, and Southeast Asia. Nation states have responded by attempting to regulate Internet discourse, undermine encryption, and expand surveillance.

In an effort to stem the tide of state overreach and protect against “netwars” and psychological campaigns, various stakeholders ranging from hacktivists to government agencies have developed computer programs that use open source and free cryptography tools to protect anonymity and bypass censorship. One such tool is the Onion Router, more commonly known by its acronym TOR, which has become virtually synonymous with the dark web. The explosion of online surveillance in the form of “Big Data” and machine learning over the past decade, along with massive data breaches that have cumulatively exposed the personal information of billions of Internet users, has led more people to seek privacy protections, including dark web tools. For instance, following the revelations by Edward Snowden of mass surveillance by the U.S. National Security Agency (NSA), TOR saw the number of daily users spike to nearly 6 million (see Figure 1).

Corporations are also taking on a greater role. On October 24, 2018, Apple’s CEO Tim Cook addressed the European Parliament, thanking Europe in taking a leading role through the General Data Protection Regulation (GDPR) and encouraging other parts of the world to follow suit. Cook argued that

Figure 1. The number of daily TOR users spikes in May 2013 following Edward Snowden's revelations of mass surveillance

Source: Used with permission from The Tor Project, Inc. under Creative Commons Attribution 3.0 United States License.



privacy was a “fundamental human right” and defended his company’s use of encryption to protect its customers (Cook, 2018). Despite pressures from governments to break encryption or provide back door access to communications, more companies have followed Apple’s lead in encrypting mobile devices, computers, and applications. Google and Facebook have embraced the Signal messaging protocol, an end-to-end encryption protocol developed by the non-profit Open Whisper Systems, as the default for Google Allo, Facebook Messenger, and WhatsApp (Cohn-Gordon et al., 2017). And new forms of encryption involving blockchain technology are being developed to protect sensitive information, such as health records, and preserve user privacy (Castaldo and Cinque, 2018).

Despite the clear benefits of protected communications in preserving privacy and human rights, some governments see encryption as a threat to national security and safety, typically citing the use of the dark net and encrypted messengers by terrorists, pedophiles, and criminal hackers. In 2018, ministers representing the Five Eyes nations (Australia, Canada, New Zealand, the United Kingdom, and the United States) met in Australia to discuss ways to combat “certain encryption designs” used to evade law enforcement. They urged “service providers to voluntarily establish lawful access solutions” or back doors to their products (Statement of Principles on Access to Evidence and Encryption, 2018). Shortly afterward, the Australian Parliament passed anti-encryption legislation titled the *Telecommunications and Other Legislation Amendment Act 2018* that requires companies to create back doors when requested. It immediately resulted in a flight of customers from the Australian tech sector (Crozier, 2019). One technology investor described Australia as “the place least welcoming to cybersecurity practitioners in the world” (McLean, 2019).

The exceptional access debate renews a defunct attempt by the NSA in the 1990s to introduce a “Clipper Chip,” ostensibly an encryption device that secured telephone communications. If implemented, a copy of the encryption keys would have been held in escrow to be used by law enforcement to wiretap select phones. However, researchers found that securing the keys in a centralized location was not only technologically challenging and expensive, it introduced security vulnerabilities that potentially undermined all secure communications (Abelson et al. 1997). For instance, the keys could be compromised by malicious insiders or through a cyberattack. The proliferation of encrypted devices since the 1990s

has only compounded the potential cost and challenges of implementing exceptional access (Abelson et al. 2015). Moreover, American companies have long argued that they would be placed at a competitive disadvantage to foreign competitors not bound by exceptional access requirements (Levy, 1994) and that only by relaxing encryption export controls in the late 1990s was the United States able to give birth to Amazon, eBay, and other firms that came to dominate global e-commerce.

The impact of Australia's anti-encryption legislation remains to be seen. However, given that the largest technology companies, including Apple, Facebook, and Google, are US-based, their underlying computer code, including encryption designs, will continue to enjoy protection under the First Amendment. Moreover, as noted in *Yahoo!, Inc. v. La Ligue Contre Le Racisme* (2001), that protection is extraterritorial if the service is provided from US-based computer networks.

Finally, the borderless nature of the Internet makes the regulation of encrypted communications nearly impossible to enforce. Technology companies will simply relocate to favorable jurisdictions, causing economic harm to countries with strong anti-encryption regulations. Brantly (2017), a Cyber Policy Fellow at the U.S. Army Cyber Institute Combating Terrorism Center argued that removing encryption from export bans in the early 1990s "was pivotal to the expansion of the internet because it made possible secure online commerce and the protection of communications and data." If the United States were to abandon its protection of computer code, and encryption in particular, it "would result in billions in lost revenues and undermine many of the core technical communities at the heart of the modern digital economy." Regulations seeking to ban or break encryption are misguided at best, he claims. Such regulations would simply increase the security risks for law-abiding citizens, while pushing criminals further underground and, by extension, making them more difficult to monitor. "Code, or the logical constructs within which encryption is implemented, is deliberate, and it functions to achieve software goals and objectives," Brantly notes. "From a technical perspective, the addition and manipulation of code that would be necessary to create backdoors undermines security."

FUTURE RESEARCH DIRECTIONS

The protection of computer code under the U.S. constitution has far reaching implications, as the world's largest technology companies are U.S.-based. However, that will not always be the case. As more technology companies emerge from other parts of the world, researchers will need to consider how to better harmonize the laws that govern computer code and the Internet. For instance, can members of the Five Eyes circumvent domestic laws by locating surveillance in a member state that does not have a Bill of Rights, like Australia? European law has already conflicted with U.S. law in *Yahoo!, Inc. v. La Ligue Contre Le Racisme*. Similarly, the GDPR is forcing companies in the U.S. to comply with European privacy regulations. Managing these conflicting laws and regulations will continue to pose challenges as lawmakers and regulators introduce new constraints.

Another important consideration is how regulations and laws have impacted innovation. For instance, First Amendment protection of computer code has been a driver of innovation that contributes to U.S. dominance in information technologies (Brantly, 2017). Will proposed regulations against encryption in other countries where computer code is not protected discourage innovation and entrepreneurship in the tech industry? Future research should consider the economic value of U.S. free speech protections of computer code and how to measure the economic impact of reversing these protections. For instance, the Information Technology and Innovation Foundation (ITIF) estimated that U.S. cloud computer companies like Google and IBM lost between \$22 billion and \$35 billion because of Edward Snowden's

NSA surveillance disclosure as companies shifted contracts away from the United States to companies in countries that promised to protect privacy, such as Switzerland and Germany (Castro, 2013).

CONCLUSION

Computer code and, by extension, cryptography are forms of speech protected by the First Amendment of the U.S. Constitution. However, the courts have also held that computer code is a special form of speech that has both functional and expressive elements. In many ways, computer code is more like art than pure speech and it can be restricted when there is a substantial government interest in doing so. Such restrictions, however, must not be more burdensome than necessary to achieve that government interest.

Governments seeking to regulate of the Internet and undermine cryptography do so on the premise that steps are needed to counter terrorists, hackers, child pornographers, and drug cartels. Some corporations have opposed what they see as government overreach, because it would undermine the security and privacy of law-abiding citizens. For instance, the NSA developed surveillance tools that gave backdoor access to Microsoft Windows servers and personal computers. Although there is no evidence that these tools prevented terrorist attacks or exposed criminal organizations, they were later leaked and weaponized by state-sponsored criminal hackers to develop powerful malware that destroyed computer networks around the world (Nakashima and Timberg, 2017). The NSA exploits caused major disruptions to the British National Health Service, crippled shipping giants Maersk and FedEx, and resulted in widespread power outages in the Ukraine. The estimated cost of the damage was in the tens of billions of dollars.

A noble purpose is not enough to warrant efforts to undermine cryptography. Leaked NSA tools demonstrate that back doors and hacking tools can fall into the wrong hands and be deployed by criminal hackers and repressive regimes to undermine democratic values. And while some agencies like the NSA and Federal Bureau of Investigation (FBI) have sought to ban or undermine encryption, other U.S. government branches, such as the U.S. military and the National Science Foundation, have been important backers of encryption and privacy tools like TOR. This support, along with the legal protections afforded to computer code under the U.S. constitution, have allowed the United States to dominate technology industries. When consumers lose confidence in these protections, it undermines the standing of American companies. Snowden's immediate impact on the economy should be viewed as a warning sign to legislators of the risks of tampering with the protections that have allowed the Internet to grow and flourish.

Today, the dark web and virtual private networks (VPNs) are used to bypass censorship in Venezuela, Russia, and China, to protect whistleblowers and journalists, who increasingly face threats to their safety and freedom, and counter what privacy activists describe as the surveillance state. News organizations have set up TOR onion sites as drop boxes where whistleblowers can anonymously submit news stories and tips, while some, like The New York Times, have created onion versions of their regular websites that can only be accessed using specialized anonymity browsers to bypass censors and evade surveillance. In western countries, the surveillance state and large corporate data breaches have created suspicion among many Internet users who are turning to encrypted messengers, VPNs, and TOR to protect their online privacy, while activists who support these services hope to force governments and corporations to be more accountable.

REFERENCES

- Abelson, H., Anderson, R., Bellare, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Schneier, B. (1997). *The risks of key recovery, key escrow & trusted third party encryption; A report by an ad hoc group of cryptographers and computer scientists*. Retrieved from <https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W>
- Abelson, H., Anderson, R., Bellare, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*. doi:10.1093/cybsec/tyv009
- Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141–165. doi:10.1080/01495939308402915
- Bar-Hillel, Y. (1951). The present state of research on mechanical translation. *American Documentation*, 2(4), 229–237. doi:10.1002/asi.5090020408
- Bar-Hillel, Y. (1953). Some linguistic problems connected with machine translation. *Philosophy of Science*, 20(3), 217–225. doi:10.1086/287266
- Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Retrieved from <https://www.eff.org/cyberspace-independence>
- Bernstein v. United States Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999)
- Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1996 U.S. Dist. LEXIS 5084, 96 D.A.R. 6721 (N.D. Cal. 1996)
- Brackbill, H. (1929). Some Telegraphers' Terms. *American Speech*, 4(4), 287–290. doi:10.2307/452061
- Brantly, A. (2017). Banning Encryption to Stop Terrorists: A Worse than Futile Exercise. *CTC Sentinel*, 10, 7.
- Broadrick v. Oklahoma, 413 US 601 (US, 1973).
- Brownson, H. L. (1953). Literature notes. *American Documentation*, 4(4), 174–184. doi:10.1002/asi.5090040406
- Camp, J., & Lewis, K. (2001). Code as speech: A discussion of Bernstein v. USDOJ, Karn v. USDOS, and Junger v. Daley in light of the US Supreme Court's recent shift to Federalism. *Ethics and Information Technology*, 3(1), 21–33. doi:10.1023/A:1011427806551
- Castaldo, L., & Cinque, V. (2018, February). Blockchain-based logging for the cross-border exchange of ehealth data in europe. In *International ISCIS Security Workshop* (pp. 46-56). Springer. 10.1007/978-3-319-95189-8_5
- Castro, D. (2013). How much will PRISM cost the US cloud computing industry? *The Information Technology & Innovation Foundation*, 1-9.
- Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2017, April). A formal security analysis of the signal messaging protocol. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on* (pp. 451-466). IEEE. 10.1109/EuroSP.2017.27

Cook, T. (2018, October 24). *Keynote address from Tim Cook, CEO, Apple Inc.* Retrieved from <https://www.youtube.com/watch?v=kVhOLkIs20A>

Crozier, R. (2019, February 14). *Aussie IT firms cop customer trust hit as encryption laws bite.* Retrieved from <https://www.itnews.com.au/news/aussie-it-firms-cop-customer-trust-hit-as-encryption-laws-bite-519286>

Ferrera, G. R. (2004). *Cyberlaw: text and cases* (2nd ed.). Mason, OH: Thomson/South-Western/West.

Hayden, M. (2016, February 25). *The Encryption Wars And Privacy Shield.* Retrieved from <https://soundcloud.com/newamerica/the-encryption-wars-and-privacy-shield>

Junger v. Daley, 209 F. 3d 481 - Court of Appeals (6th Cir., 2000).

Karn v. United States Dep't of State, 925 F. Supp. 1, 1996 U.S. Dist. LEXIS 5707 (D.D.C., 1996).

Levy, S. (1994, June 12). *Battle of the Clipper Chip.* Retrieved from <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all>

Madsen, W., Sobel, D. L., Rotenberg, M., & Banisar, D. (1997). Cryptography and liberty: An international survey of encryption policy. *The John Marshall Journal of Computer & Information Law*, 16, 475.

McLean, A. (2019, March 13). *Australia isn't buying local cyber and the rest of the world might soon follow.* Retrieved from <https://www.zdnet.com/google-amp/article/australia-isnt-buying-local-cyber-and-the-rest-of-the-world-might-soon-follow/>

Nakashima, E., & Timberg, C. (2017). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loosethen-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

Reno v. American Civil Liberties Union, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997).

Roth v. United States, 354 U.S. 476, 484, 77 S.Ct. 1304, 1 L.Ed.2d 1498 (1957).

Statement of Principles on Access to Evidence and Encryption. (2018, August 29). Retrieved from <https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption>

United States v. O'Brien, 391 U.S. 367 (1968). *Yahoo! Inc. v. La Ligue Contre Le Racisme*, 169 F. Supp. 2d 1181 - Dist. Court, (ND Cal., 2001).

Zetter, K. (2017, June 3). *Tor Hires a New Leader to Help It Combat the War on Privacy.* Retrieved from <https://www.wired.com/2015/12/tor-hires-a-new-leader-to-help-it-combat-the-war-on-privacy/>

ADDITIONAL READING

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *The Journal of Economic Perspectives*, 31(2), 211–236. doi:10.1257/jep.31.2.211

Howard, P. N., & Hussain, M. M. (2013). *Democracy's fourth wave?: digital media and the Arab Spring*. Oxford University Press. doi:10.1093/acprof:oso/9780199936953.001.0001

Kerr, O. S. (2000). The fourth amendment in cyberspace: Can encryption create a reasonable expectation of privacy. *Connecticut Law Review*, 33, 503.

Lichtblau, E., & Benner, K. (2016). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*, 17.

Mitnick, K. D., Vamosi, R., & Hypponen, M. (2017). *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of Big Brother and big data*. New York: Little, Brown and Company.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 58(1), 7–38. doi:10.1080/00396338.2016.1142085

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. PublicAffairs.

Simmons, B. A. (2009). *Mobilizing for human rights: international law in domestic politics*. Cambridge University Press. doi:10.1017/CBO9780511811340

Syverson, P., Dingedine, R., & Mathewson, N. (2004). Tor: The second generation onion router. In Usenix Security.

KEY TERMS AND DEFINITIONS

Blockchain: An encrypted ledger that protects transaction data from modification.

Cleartnet: Mainstream websites that are indexed by popular search engines, like Yandex, Google, and Bing.

Dark Web: A part of the deep web that uses hidden services to promote anonymity and prevent unauthorized access.

Deep Web: Internet sites that are not indexed by mainstream search engines. It can include password protected networks, such as corporate networks, email, and subscription only newspapers.

Encryption: A form of cryptography that protects data from being viewed without a decryption key.

GDPR: The General Data Protection Regulation is a European regulation that governs the protection of data and right to privacy of European citizens and residents.

Onion: A hidden Internet domain that disguises a site's true Internet (IP) address. Onion domains are accessed using TOR, usually through a specially designed Internet browser.

TOR: The Onion Router is an Internet protocol that uses multiple encrypted relays to protect user anonymity.

The TOR Browser: An Internet browser that is specially designed to use TOR to access both dark web and cleartnet sites.

Virtual Private Network (VPN): A remote server that creates an encrypted connection between the client and server to protect access.

Cybersecurity Legislation

Christopher Thomas Anglim

University of the District of Columbia, USA

INTRODUCTION

Nations throughout the world use cyberspace legislation to protect their cybersecurity and control criminal activity on the Dark Web. The Dark Web consists of underground websites and databases that are accessible anonymously using “The Onion Router” (TOR). Development of the technology operating TOR has frequently been attributed to the US Naval Research Laboratory. TOR protects the user’s identity by routing ordinary location services and Internet Protocols (IPs) through several different nations. TOR is an example of a darknet, which is a closed, private network that operates on the more conventional Internet Protocols. Darknets bypass the TCP/IP to ensure anonymous, essentially untraceable global networks.

The US government had intended to use TOR to provide the means for activists in nations with repressive governments to communicate with each other, without their government becoming aware of their activities. TOR has, however, become a form of contemporary technology that provides criminals with swift and often anonymous means to move funds and goods to enrich themselves through a wide variety of illegal activities such as hosting malware, selling illicit drugs, disseminating child pornography, arranging for contract killings, conducting terrorist acts, and laundering money.

This chapter explains the role of the legislature on all levels in controlling criminal behavior on the Dark Web, including the purpose of cybersecurity legislation, different approaches legislation, and the benefits and limitations of the legislative approach. In the United States, Congress continues to consider federal legislation intended to control the widespread criminal behavior that occurs on the Dark Web, such as the sale and distribution of drugs, illegal weapons, and child pornography. This chapter begins with an introduction that explains the purpose behind legislation. This followed by the Background section, which provides an overview on the topic of Legislation and the Dark Web, the purpose of such Legislation. Because this topic involves the balancing of basic rights and duties, the section also discusses the constitutional issues involved. Much of the chapter deals with Congressional action to date on the Dark Web and what Congress still needs to do on this topic. The Chapter then discusses legislative action taken on the state level, the international level, and legislative action that other nations have taken. The chapter concludes with recommendations for creating a legislative regime that seeks to both control criminal behavior on the Dark Web and ensure that the Dark Web is available for those who use need it for legitimate purposes.

Understanding Legislation as Lawmaking

Legislation is law as enacted by a legislative body after it has considered a specific measure. Laws enacted by Congress, a parliament, a state legislature, or a city council are examples of legislation. In the American system, legislation usually becomes law after being approved by an executive (such as the President, Governor, or Mayor) or if the legislature overrides the executive’s veto.

Legislation reflects policy considerations, meaning that it is subject to political concerns and preferences. The executive branch implements legislation and the judiciary reviews legislation. All laws require balancing between the individual's right to privacy and protecting the public's right to be protected. Liberty rights, including privacy rights are not absolute. These rights are balanced by the rights of other individuals and society. For nearly 30 years, legislatures on the local, state, and federal government have sought to prohibit certain types of behavior using computers as "cyber-crimes". This means that a government will prosecute individuals for violating the law and has imposed specific sanctions (such as fines and prison terms) for these violators.

As a very new type of law, cyberspace law remains a work in progress. While the principles of cybersecurity law are derived from the law governing other legal areas, not all of these precedents are designed to fit the current reality of cybersecurity. The Dark Web, especially, poses a large number of legislative challenges. These involve difficult issues of balancing the protection of free speech rights of individuals versus the need to protect the community from the online trade in a whole variety of illegal goods and services. Some of the many challenges in drafting cybersecurity law include that criminals freely use technology to maintain anonymity on the Web. This allows them to evade law enforcement with relative ease. The need for legislative action in controlling criminal activity on the Dark Web became particularly apparent as law enforcement agencies uncovered such sites as the "Silk Road", which were anonymous online markets for illicit and illegal goods. These online black markets allowed buyers to purchase illegal drugs and the transactions in bitcoin and conduct transactions anonymously, using "dummy" transactions to conceal the connection between buyers and sellers. By so doing, the Silk Road evaded The US's most advanced electronic surveillance technology. The site operated from 2011 until the Federal Bureau of Investigations (FBI) curtailed its operations in 2013. While in operation, the Silk Road amassed an estimated \$1.2 billion in revenue. Other illicit sites such "Pandora Market" and "Hydra Marketplace" followed the Silk Road Model.

The situation has worsened grew worse over time. At the time law enforcement authorities force the site, Alpha Bay to close in 2017, that site had 200,000 users, 40 vendors, and was ten times the size of Silk Road. Alpha Bay indicated that buyers and sellers were scaling up their operations on the Dark Web.

At the same time, hackers operating in the Dark Web stole a large amount of private customer data from Equifax, a major consumer credit reporting agency. The hackers then demanded 600 Bitcoins (about \$2.5 million) in exchange for the sensitive financial information of the 143 million people. The way that these criminals were able set up such a secret, untraceable criminal enterprise at such a massive scale led policymakers to doubt whether law enforcement had sufficient authority and technology to contend with the illicit Dark Web activities (Ghappour, 2017).

The Dark Web has also become a major marketplace of counterfeit and stolen medicine. Criminals have found that the return on investment of such products has been very high. This trade in harmful, useless, or expired medicines has tragically led to the deaths of many who relied on them.

BACKGROUND

Overview

Cyberspace is a virtual computer world. More specifically, is an electronic medium used to form a global computer network to facilitate online communication. This chapter focuses on recent cybersecurity legislation, seeks to determine the effectiveness of specific cybersecurity legislation, and present

possible alternative policy alternatives. This chapter focuses on: 1) the scope of cyberspace legislation, 2) the rationale for cyberspace legislation, 3) arguments in favor of certain cyberspace legislation, 4) arguments against certain cyberspace legislation, 5) the evolution of cybersecurity legislation, 6) the impact and effectiveness (or likely impact and effectiveness) of this legislation and 6) what additional cybersecurity legislation might be necessary, both on the state and federal level. Specifically, this chapter discusses legislation intended to control criminal behavior on the Dark Web. One should note that there are three types of law: statutory law (law passed by a legislature), case law (law promulgated by the courts), and administrative law (law issued by an administrative agency). In terms of scope and definition, cyberspace legislation is law on cyberspace passed by a legislature (such as Congress on the federal level and state legislatures on the state level). Legislation does not become binding and effective until signed by the jurisdiction's chief executive (such as the President of the United States or the Governor of an American state).

Cyberspace law is intended to both control criminal behavior on the deep web, while also protecting legitimate speech and legitimate business transactions. In efforts to control criminal behavior on the Dark Web, there is the possibility that legislation directed against the Dark Web may also adversely affect the flow of information among peoples living in oppressive regimes, where information is heavily censored. In addition, the military, corporate whistleblowers, and victims of abuse need access to the Dark Web to both maintain their confidentiality while exercise their free speech rights.

A recent British study analyzed several websites accessible through TOR and found that 1,547 out of 2,723 live sites had "illicit content" (Moore & Rid, 2016). Usually this content included "drugs, illicit finance and pornography involving violence, children and animals" (Moore & Rid, 2016). The researchers concluded that "more than 50 per cent of what's hosted [on TOR] is illegal and illegitimate", while other reports found that an even higher representation. The researchers explained that the discrepancy is due to the fact that they used a restrictive definition of illicit content (McGoogan, 2016). The actual representation, however, may be even higher because the researchers did not review every Dark Web site because of how TOR operates (Moore & Rid, 2016). Nonetheless, the researchers presented much evidence that the Dark Web facilitates criminal behavior on a massive scale. Further, the researchers show that law enforcement agencies have serious difficulties in identifying and prosecuting the accused.

Legislating against criminal behavior on the Dark Web entails the difficult objective of ensuring an equitable balance between individual liberty and public safety. The key issues include: 1) Who should police the Dark Web and what authority should they have?, 2) What is the scope of authority of those who police the Dark Web?, 3) What are the benefits of an international agreement and organization to police criminal behavior on the Dark Web.

Browsers on the Dark Web provide users complete anonymity, which help criminals conduct their trades largely undetected. While potential enforcement options exist, each have drawbacks. Some commentators argue that crime on the Dark Web can only be truly eradicated by completely eliminating the entire Dark Web (Haasz, 2016). James Clapper, the former Director of the National Security Agency is one of those who favors eliminating online anonymity because America's adversaries use it to direct attacks against the United States and its allies throughout the world.

Despite the risk involved, there is a large volume of both legitimate and illicit goods and services bought and sold on the Dark Web, with an always available supply of willing sellers and willing buyers (Haasz, 2016). The only feasible solution, then may be to enact effective legislation crafted to deter crime and improved enforcement of criminality on the Dark Web.

Michael Chertoff, a former Secretary of the Department of Homeland Security during the George W. Bush administration, well described the challenges of drafting legislation intended to protect against criminal behavior on the Dark Web:

Creating policy to address the Dark Web requires an understanding of the benefits and risks of anonymity and of an open internet. Rash and sweeping legislation has the potential to encroach on civil liberties and to be a nightmare to enforce. On the other hand, not addressing the Dark Web will allow illicit activities to persist unabated. It is impossible to regulate the Dark Web in isolation; any regulations must be applicable to the internet as a whole and will thus affect Surface Web users, Deep Web researchers, and Dark Web criminals alike (Chertoff, 2017).

Defining the Purpose of Cybersecurity Legislation

Cybersecurity legislation reflects the legislature's intent to protect the American people against cyber-criminals who seek to exploit perceived and actual cyber-vulnerabilities. These cyber- vulnerabilities exist within the critical infrastructure information environments worldwide. Cyber-vulnerabilities include flaws in computer systems or set of procedures that could create a threat. Threats to the international cyber infrastructure continues to escalate and diversify. Thus, these vulnerabilities present ubiquitous challenges to governments, businesses, political organizations, and individuals. The criminal attackers are often motivated by a wide variety of differing purposes, including seeking military intelligence, diplomatic or commercial espionage, cybercrime, or achieve political advantage. Legislators, then, must consider these threats in seeking to draft such cyberspace legislation.

Constitutional Concerns Involved With Federal Cybersecurity Legislation

As with all federal legislation in the United States, the legislation against criminal activities on the deep web must be comply with relevant provisions of the US Constitution. Of these provisions, the Fourth Amendment is particularly important. The Fourth Amendment protections against the unreasonable search and seizure, by any government entity, of one's person or one's property by requiring that a warrant based upon probable cause be issued by a neutral magistrate. A 'search' occurs when the government infringes on what society views as a reasonable expectation of privacy. Courts recognize that certain areas such as an individual's home have the highest level of privacy protection. The Fourth Amendment, for example, strongly protects against a warrantless search of a person's home, while providing much less protections in other areas. Contemporary technology greatly complicates privacy protection under the Fourth Amendment particularly because American law has not kept pace with the changing social expectations of privacy. For many contemporary Americans, their most smartphones and laptops hold their most confidential information and could cause much damage if they fall into the wrong hands (Ghappour, 2017).

The American Approach to the Statutory Law of Cyberspace

For over two decades, US cybersecurity policy approach has developed largely based on self-regulation and incremental improvement, following Thomas Kuhn's "change theory". Under this theory, a change from one paradigm to another occurs when sufficient issues occur under the current paradigm develop, forcing reasonable observers to question the existing order. It remains controversial as to whether this

interpretation of change theory is sufficient to meet current need to ensure cybersecurity due to the dynamic challenges posed by nature of illicit behavior on the Dark Web. Nonetheless, change theory continues to form the basis of existing American federal Cyberspace law.

Congressional Action on Cybersecurity

As the national legislature, Congress has a critical role in articulating and protecting federal cybersecurity. Most federal cybersecurity statutory law was enacted prior to 2002. Because of several obstacles in crafting effective legislation on criminal activities on the Dark Web, Congress has enacted very little legislation on that topic. Nonetheless, Members of Congress continue to be highly interested in the topic, as evidenced by the large amount of debate and legislation introduced on the topic. The question is, then, why has a major federal statute not been enacted on criminal behavior on the Dark Web. What legislation Congress has actually enacted delegates much of the federal legal authority over activities on the Dark Web to certain federal agencies, which regulate these activities through their rulemaking and enforcement powers. This delegation is justified in part because these agencies have the expertise needed to make such regulations.

In 2002, Congress enacted the Homeland Security Act (HSA, 2002) and the Federal Information Security Management Act (FISA, 2002). HSA is foundational legislation that stipulates the roles and responsibilities for federal cybersecurity protection. It also required agencies to develop and implement programs to secure their information and information systems. In 2004, Congress enacted the Federal Information Security Modernization Act (FISMA, 2014). This modified the original 2002 statute to clarify and update the responsibilities and authorities of DHS and the US Office of Management and Budget (OMB) to protect federal agency information security. In recent years, Congress has considered legislation to expand DHS's cybersecurity authority. In 2014, Congress enacted the National Cybersecurity Protection Act of 2014 (NCPA, 2014), which codified the National Cybersecurity and Communications Integration Center (NCIC) within DHS to interface and share cybersecurity information across federal and non-federal entities (including the private sector). Also in 2014, Congress enacted the Federal Information Technology Acquisition Reform Act (FITARA) of 2014 to expand the authority of chief information officers (CIOs) and deal with issues including risk management, IT training, and acquisition/procurement. In 2015, Congress passed the Cybersecurity Information Sharing Act (CISA) (CISA, 2015) which authorized the US Department of Homeland Security (DHS) to exchange threat information with the private sector. Congress, at that time, however, declined to grant DHS complete authority over cyberspace. It recognized the authority of other agencies over cyberspace issues and allowed them to continue asserting control over cybersecurity in the civilian sector. Several Congressional committees claim jurisdiction over DHS and argue that they should be the committee that should have jurisdiction to protect federal cyberspace policy.

Congress enacted CISA (CISA, 2015) to encourage federal government and private industry to share information, through DHS, by providing liability protections for private individuals and organizations that share relevant information with DHS. CISA also requires all federal non-defense agencies to implement EINSTEIN, a DHS program that detects and blocks threats to federal networks.

On December 12, 2017, President Barack Obama signed the National Defense Authorization Act (NDAA) for Fiscal Year 2018 (NDAA, 2017). This statute launched several cybersecurity initiatives and new rules and programs on information security, including formally prohibiting use of Kaspersky Lab software (NDAA, § 1634, 2017), granting the President authority to define cyberwar" (NDAA, § 1633,

2017), and mandating the Department of Defense to evaluate and reorganize its internal organizational structure to implement cybersecurity and related missions (NDAA, §§ 1641, 1644, et al., 2017).

On August 13, 2018, Congress enacted the National Defense Authorization Act (NDAA) for Fiscal Year 2018, which authorized appropriations and US Defense Department policies on issues such as cybersecurity and the Dark Web. Some privacy advocates have argued that some federal cybersecurity statutes may encourage more individuals to rely on the Dark Web. Congress, under the Trump Administration, for example, passed legislation to strengthen the federal surveillance power over the computer behavior of Americans on the basis of national security. In March 2018, President Trump signed into law the “Clarifying Lawful Overseas Use of Data Act (CLOUD, 2018)”, which abolished an Obama-era privacy rule that prohibited Internet Service Providers (ISPs) from sharing user information without their consent. Privacy advocates argued that this may encourage more Internet users to rely on the Dark Web to protect their identity.

A similar debate, also in the Spring of 2018, occurred when Congress voted to approve legislation to discourage advertising for prostitution on the Internet by making websites more responsible for the ads and postings that appear on their sites. Congress did this by amending Section 230 of the Communications Decency Act of 1996 (which is intended to protect free speech on the Internet) (CDA, 1996). Some members of Congress supported amending the section after the adult-services website, backpage.com, successfully used the section to defend itself in court for posting ads for child prostitution. Proponents of the law raised the case of Desiree Robinson, a 16 year old young woman, who aspired to be an Air Force doctor. She was killed by a man who paid for sex with her after seeing an ad paid by Desiree’s pimp was placed on backpage.com. Some privacy and free speech groups argued that this decision would make involuntary sex workers more vulnerable by forcing prostitution increasingly into the Dark Web. The became law and specifically provided that Section 230 does not prohibit enforcement against providers and users of interactive computers and services, of federal and state criminal law relating to sexual exploitation of children or sex trafficking (Allow States and Victims to Fight Online Sex-Trafficking Act, 2017).

While there is some federal statutory law applicable to Dark Web, these statutes were never specifically drafted to meet the special challenges of the Dark Web. The Dark Web, for example, facilitates hacking and aids hackers. Hackers often obtain their malware from other hackers, or seek to extort money through ransomware. In cases such as these, the Computer Fraud and Abuse Act (CFAA), has been interpreted as prohibiting hacking a form of trespassing on, unauthorized accessing of, and damaging computers in interstate or international commerce. The CFAA also bars trafficking, unauthorized computer access, and computer espionage. While these U.S. statutes may adequately cover hacking, they do not address the issues of anonymous online users. They also do not effectively prosecute Dark Web criminal activities emanating from outside the United States, where most cybercrime directed against the United States originates from. Because of this, effective international action and cooperation is essential in addition to effective, well-drafted US federal legislation to confront criminal behavior on the Dark Web (Chertoff, 2017).

State Cybersecurity Legislation

Cybersecurity threats have serious implications for government security, economic prosperity and public safety. State governments address cybersecurity issues by actions such as: 1) requiring government or public agencies to implement security practices; 2) offering incentives to cybersecurity; 3) providing

exemptions from public records laws for security information; and 4) creating cybersecurity commissions, studies or task forces.

State Efforts to Promote Cybersecurity Training and Education

Like the Federal government, state governments address cybersecurity through various approaches. On the state level, these initiatives include requiring government or businesses to implement security procedures or security audits, creating studies or task forces, and promoting the cybersecurity industry or training for technology skills.

States address cybersecurity through various initiatives, including increasing funding for improved security measures, requiring government agencies or businesses to implement specific types of security practices, increasing penalties for computer crimes, and addressing threats to critical infrastructure. In recent years, most state legislatures have deliberated cybersecurity or data security, while some governors issued executive orders.

Many of these bills considered matters related to: 1) security practices and protection of information in government agencies, 2) exemptions from state Freedom of Information of Public Records acts for information that could jeopardize security of critical information or infrastructure, and 3) cyber/computer crimes.

These statutes are intended to: 1) Improve government security practices, 2) Create commissions, task forces and studies, 3) Provide funding for cybersecurity programs and initiatives, 3) Target computer crimes, 4) Restrict public disclosure of sensitive security information, and, 5) Promote workforce, training, economic development.

Cyberattacks Against United States Targets

Numerous diverse cyberattacks against US individuals and entities have ranged from corporate hacks and credit-card scams to Russian hackers and government breaches. Many of these incidents have been massive and have the potential to cause widespread devastation if successful. To prepare for the possibility of such attacks or to effectively respond to such attacks if they should occur, state and federal legislators have made cyber-safety a major legislative priority.

Much of America's cybersecurity legislative framework had been developed by 2002, well before criminal activity on the Dark Web became so prominent and pervasive. Legislative action has rapidly expanded since that time because of the continuing, changing, and growing threat to American cybersecurity, including that emanating from the Dark Web. In 2017, Congress considered over 240 federal cybersecurity bills. Once in power, the Trump Administration very quickly responded to the threat to American cybersecurity by issuing Executive Order 13800 ("Strengthening Cybersecurity of Federal Networks and Critical Infrastructure") (EO, 2017, Jul. 12) to provide more stringent data regulation and to enhance American defenses against cyberterrorism.

RECOMMENDATIONS

The American Federal cyberspace statutory framework remains largely underdeveloped. Much of this is due to the fact that there is a lack of consensus as to the legislative approach to be taken against criminal activity on the Dark Web. Although Congress has deliberated several different bills on the subject, it

remains challenging to craft effective legislation that both prohibits illicit activity on the Dark Web and does no beneficial, useful, and lawful activity that also occurs on the Dark Web. Both state legislation and caselaw on the criminal activity on the Dark Web should help inform further development of federal legislation on the subject. Congress continues efforts to develop comprehensive federal legislation, appropriately designed to protect individual Americans and American entities in cyberspace. Federal legislation, thus, should have the following provisions that both to protect against criminal behavior on the Dark Web and protect against individual liberty.

1. The purpose of the legislation and the definition of the offenses and penalties pertaining to the criminal activities on the Dark Web.
2. Contain language to help protect freedom of speech, creative innovation, and legitimate economic transactions through the Internet.
3. Clearly delineate the duties and responsibilities of government agencies charged with combatting criminal activity on the Dark Web.

Despite how federal law evolves in protecting against criminal activity on the Dark Web, it must do the guarantee four key objectives: 1) protect the civil rights, civil liberties and privacy rights of Americans, 2) maintain a lawful means of accessing encrypted data to facilitate criminal investigations, 3) gather effective, relevant intelligence, and 4) protect Americans and American entities against criminal activity on the Dark Web.

It is also be instructive to see how other nations draft legislation on the Dark Web. Germany, for example, is considering criminalizing the provision of Dark Web infrastructure providers and making such actions punishable by three years in prison. Civil libertarians and journalists are among those who oppose this legislation.

CONCLUSION

All Legislators (whether serving on the international, national, state, or local levels) are concerned about criminal activity on the Dark Web and the harm that individuals and organizations could suffer as a result of this behavior. The legislator's work is challenging because 1) he or she must balance the needs of individual liberty and privacy versus the need to protect public safety, and 2) the Dark Web is an international phenomenon, which transcends national boundaries, national laws, and national enforcement. Thus, in addition to well-drafted national legislation, then, there must also be both effective international legal standards and international cooperation to combat the criminal use of the Dark Web.

REFERENCES

- Allow States and Victims to Fight Online Sex-Trafficking Act of 2017 (2018), Pub. L. No. 115-164, 132 Stat. 1253.
- Chertoff, M. (2017). A Public Policy Perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), 26–38. doi:10.1080/23738871.2017.1298643
- Clarifying Lawful Overseas Use of Data Act (CLOUD) (2018). Pub. L. No. 115-141, 132 Stat. 348.

- Communications Decency Act of 1996 (CDA) (1996). Pub.L. No. 104-104, 110 Stat. 56.
- Computer Fraud and Abuse Act (CFAA) (2018), Pub.L.No. 99-474, 100 Stat. 1213, 18 U.S.C. § 1030.
- Cybersecurity Information Sharing Act (CISA) of 2015. S. 114-754 (2015).
- Executive Order 13800 (“Strengthening Cybersecurity of Federal Networks and Critical Infrastructure”) (2017, Jul 12). *Federal Register*, 82, 32172-32174.
- Federal Information Security Management Act (FISA, 2002), Pub. L. No. 107-347, 116 Stat. 2899.
- Federal Information Security Modernization Act (FISMA) (2014). Pub. L. No. 113-283, 128 Stat. 3076.
- Ghappour, A. (2017). Searching Places Unknown: Law Enforcement Jurisdiction On the Dark Web. *Stanford Law Review*, 69, 1075.
- Haasz, A. (2016). Underneath it All: Policing International Child Pornography on the Dark Web. *Syracuse Journal of International Law and Commerce*, 43, 353–378.
- Homeland Security Act (HSA) (2002). Pub. L. No. 197, 116 Stat. 2135.
- McGoogan, C. (2016, February 2). *Dark web browser Tor is overwhelmingly used for crime, says study*, Retrieved from The Telegraph: <http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/>
- Moore, D., & Rid, T. (2016). *Cryptopolitik and the Darknet*. Retrieved from Taylor and Francis Online Vol. 58 (2016): <http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>
- National Cybersecurity Protection Act of 2014 (NCPA) (2014). Pub. L. No. 113-282, 128 Stat. 3066.
- National Defense Authorization Act (NDDA) for Fiscal Year 2018 (2018). Pub. L. No. 115-191, 132 Stat. 1253.

ADDITIONAL READING

- Cybersecurity Litigation. (2017). *Cybersecurity Law*, 51-104. doi:10.1002/9781119231899.ch2
- Dallins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation*, 24, 62–71. doi:10.1016/j.diin.2017.12.003
- Grady, M. F., & Parisi, F. (2011). *The law and economics of cybersecurity*. New York: Cambridge University Press.
- Kosseff, J. (2017). *Cybersecurity law*. Hoboken, NJ: John Wiley & Sons. doi:10.1002/9781119231899
- Oversight of the Cybersecurity Act of 2015: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives, One Hundred Fourteenth Congress, second session, June 15, 2016.* (2017). Washington: U.S. Government Publishing Office.
- Pavlik, K. (2017). Cybercrime, Hacking, And Legislation. *Journal of Cybersecurity Research*, 2(1), 13–16. doi:10.19030/jcr.v2i1.9966

Rhodes, J. D., & Litt, R. S. (2018). *The ABA cybersecurity handbook: A resource for attorneys, law firms, and business professionals*. Chicago, IL: ABA Publishing, American Bar Association.

Tehan, R. (2015). *Cybersecurity: Legislation, hearings, and executive branch documents*. Washington, DC: Congressional Research Service.

Westby, J. R. (2013). *Legal guide to cybersecurity research*. Chicago, IL: American Bar Association, Section of Science & Technology Law.

KEY TERMS AND DEFINITIONS

Congress: A national legislative body, especially that of the US. The US Congress, which meets at the Capitol in Washington DC, was established by the Constitution of 1787. It is composed of the Senate and the House of Representatives.

Cyber-Vulnerabilities: A flaw in a computer system that can make the system vulnerable to attack. A cyber-vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Cybercrime: Any criminal action perpetrated primarily through the use of a computer.

Cybersafety: Is the safe and responsible use of Information and Communication Technologies (ICT). NetSafe's approach to cybersafety is founded on: Maintaining a positive approach about the many benefits brought by technologies. Encouraging the public to identify the risks associated with ICT.

Cybersecurity: The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Cyberspace: The domain of the worldwide technology environment.

Dark Web: The deep is a small part of the deep web that has been intentionally hidden and is inaccessible through ordinary web browsers. Internet users are unable to access this portion of the web without using browsers dedicated to providing absolute anonymity to users. The dark web has become a haven for criminal activity.

Deep Web: The part of the web not a part of the surface web. It includes content inaccessible through the use of a search engine. These include private servers that only those with permission may access, intranets utilized by a variety of organizations, or even typical social media pages that users wish to keep concealed from the general public.

Legislation: Law enacted by a legislature.

Legislature: A body of individual persons empowered to legislate; specifically, an organized body authorized to make laws for a political entity such as a nation, state or province, or a city.

Surface Web: Web content that can be indexed by ordinary search engines such as Google or Yahoo.

International Context of Cybercrime and Cyber Law

Tansif Ur Rehman

University of Karachi, Pakistan

INTRODUCTION

It is clearly evident that as people become more dependent on technology, they become easier targets of cybercrime, as it also could evolve to bring about new problems. It is also important to realize to what extent it is understood by common people that either they are really a victim or can be the victim of a cybercrime.

This research includes significance as well as international aspects of cyber laws, initiatives by the EU, USA, China, and the role of international forum for cybercrime. At the very least, it demonstrates the fact that cybercrime attacks are an almost routine form of criminality and most internet users are likely to face an attack on a daily basis.

OBJECTIVES

1. To highlight the significance of cyber laws.
2. To highlight the international aspects of cyber laws.
3. To discuss the initiatives taken by the EU, USA, and China regarding cybercrime.
4. To discuss the role of international forum for cybercrime.

BACKGROUND

Cybercrime has so advanced that it was reported in August 2018 during the Black Hat and Def Con Hacking Conference that, it was possible to even hack patients' vital signs, pacemaker, and insulin pumps in real time (Smith, 2018). Symantec, one of the leading software firms that operates antivirus and firewall packages, stated in their 'Internet Security Threat Report 2011' (published in 2012) that there had been an 81% increase in malicious attacks that they had identified, with an estimate of attacks being placed over 5.5 billion.

A Barkly sponsored survey of 660 IT companies and professionals by Ponemon Institute, USA (2018) 'State of Endpoint Security Risk' has revealed that 64% of organizations experienced successful endpoint attacks. This survey has also revealed zero-day and fileless attacks that cost millions to organizations, i.e. costs doubling for Small and Medium-sized Businesses (SMBs).

Cybercrime's pace globally is on a high rise. It is an offense that is even harder to identify and resolve as compared to traditional crimes in the international context. Cybercrime cells all around the world receives thousands of complaints on a daily basis.

DOI: 10.4018/978-1-5225-9715-5.ch028

Cyber criminals are honing their skills, while consumers remain unconcerned. Cyber criminals are innovative, organized, and far sophisticated (Hutchings, 2013). They employ their tools effectively, working harder, and focused to uncover new vulnerabilities as well as escape detection. The ICTs are opening a whole new world of opportunities for criminals and the risk remains largely unknown.

The protection against cybercrime largely depends upon the security culture adaptation by government authorities of every networked country, business organizations, and most importantly, every internet user. Prevention will always be the first and best line of defense along with radical changes in policing and legislation (Glenny, 2012). Education and awareness across the citizens will go a long way to prevent individuals against many types of cybercrime and will reduce pertinent risks (Lusthaus, 2012).

FOCUS OF THE ARTICLE

This article focuses on the significance, international aspects of cyber laws, initiatives by the EU, USA and China, and the role of the international forum for cybercrime. This research will also help to understand the computer-related crime advancement, and how to use it as defined within the premises of law in an international context.

CHARACTERISTICS OF CYBERCRIME

1. Scale
2. Accessibility
3. Anonymity
4. Portability or Transferability
5. Global reach

VARIETIES AND SKILLS OF CYBERCRIME

1. Hacking of Computers
2. Denial of Service Attacks (DoS)
3. Distributed Denial of Services Attacks (DDoS)
4. Malware
5. Spyware
6. Offense Relating to Data
7. Destroying, Disclosing, and Accessing Data
8. Misconduct in a Public Office
9. Phishing
10. Pharming
11. Hate and Harm

CYBER FRAUD

There are other crimes that use technology, i.e., fraud, which is sometimes known as cyber fraud when it is committed online (Yar, 2013). Fraud based behavior exists online as well as offline, but the internet now provides ample opportunities to use it in the form of a new tool (Ekblom, 2014). There is a wide difference regarding the victimhood of fraud. It could possibly range from buying a non-existent item from the internet to MNCs losing millions of dollars annually (Sandwell, 2010).

CYBERTERRORISM

A popular definition of cyberterrorism is the “intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber system, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil order, or significant harm” (Jones, 2005, p.4).

Terrorism is generally seen as an attack against the state’s interest, sometimes it even involves attacks against private industry. The term itself is easily understood, it consists of ‘cyberspace’ and ‘terrorism’ combination to produce the importance of terrorism that takes place either in, or through the internet.

Terrorists have used the internet, specially, from the last decade and this is perhaps a convenient way of reaching a large audience (Brenner, 2014). The main uses of the internet by terrorists are:

1. Propaganda
2. Fundraising
3. Information Dissemination
4. Secure Communication

SIGNIFICANCE OF CYBER LAWS

Yoshio Utsumi was the former Secretary General of International Telecommunication Union (ITU) from 1998 to 2006. ITU is a specialized agency of the United Nations. It is responsible for issues that concern Information and Communication Technologies. He accentuated the significance of immediate measures for security of cyberspace, Information and Communication Technology Systems (ICTs), and its infrastructure. As, the interlinking of business processes and economic activities through the use of information technology is increasing exponentially.

He further expressed his concerns regarding the instillation of consumer confidence in online activities like e-governance, commerce, telemedicine, trade, as well as hosting of various other applications. He also pointed out that cyber security is indispensable for the future development of economical as well as social activities worldwide.

According to Norton Cybercrime Report 2011, a cyber security firm, cyber crimes have increased dramatically over the years which cause the sufferings to 431 million victims globally or 14 victims every second. There are around one million cybercrime victims every day.

Findings by a research organization, Comparitech, Mr. Paul Bischoff (2018) claims that stock prices are adversely effected by data breaches. In case of a data breach, it can lead to around 0.5 percent decrease in a firm’s overall share in market.

A new study, conducted by Bromium and Dr. Michael McGuire, senior lecturer in criminology at the University of Surrey in England, presented at the RSA Conference 2018 in San Francisco has found that the cybercrime economy has grown to \$1.5 trillion dollars annually. Cybersecurity Ventures is world's renowned research company with regards to global cyber economy as well as cyber security. In their official annual Cybercrime Report 2017 they predicted that cybercrime will cost the world around \$6 trillion annually by 2021.

Cyber law can be termed as the carrefour of developing innovative technology and prescribed rule of conduct or action enforced by the controlling authority. Cyber law is an umbrella term which encircle a wide range of political and legal aspects related to the internet usage and ICT (Information and Communication Technology), which includes freedom of expression, online privacy, intellectual property, and jurisdiction, etc.

The escalation of cybercrime is so significant and impacting that cyber law has been a major concern of governments worldwide. Continuous development in cyber law tend to contend more definitive, safe, and uncluttered cyberspace. The development of regulated code of conduct for IT and other electronic medium related to it is an ongoing process to meet the evolving facets of cybercrime.

CYBERCRIME STATISTICS

According to Alvarez Technology Group (2018); Devon Milkovich (2018); and Patrick Nohe (2018) these are few of the most alarming cybercrime statistics:

1. 95% of breached records came from only three industries worldwide, government, retail, and technology.
2. There is a hacker attack every 39 seconds in US alone according to the study conducted by the Clark School at the University of Maryland, USA.
3. 43% of cyber attacks target small business. 64% of companies have experienced web-based attacks. 62% experienced phishing & social engineering attacks. 59% of companies experienced malicious code and botnets and 51% experienced denial of service attacks.
4. The average cost of a data breach in 2020 will exceed \$150 million according to Juniper Research data.
5. Since 2013 there are 3,809,448 records stolen from breaches every day.
6. According to the Q2 2018 Threat Report, Nexsuguard's quarterly report, the average distributed denial-of-service (DDoS) attack grew to more than 26Gbps, increasing in size by 500%.
7. Approximately \$6 trillion is expected to be spent globally on cyber security by 2021.
8. Unfilled cyber security jobs worldwide will reach \$3.5 million by 2021.
9. By 2020 there will be roughly 200 billion connected devices, which means more exposure to cybercrime.
10. 95% of cyber security breaches are due to human error.
11. Only 38% of global organizations claim they are prepared to handle a sophisticated cyber attack.
12. Total cost for cybercrime committed globally has added up to over \$1 trillion dollars in 2018.

TOP 10 COUNTRIES FACING CYBERCRIME

According to Sumo3000, Enigma Software Group, USA (2018), following are the top ten countries that are facing cybercrime. These 10 countries face around 63% of the total cybercrime committed across the globe.

1. USA (23%)
2. China (9%)
3. Germany (6%)
4. Britain (5%)
5. Brazil (4%)
6. Spain (4%)
7. Italy (3%)
8. France (3%)
9. Turkey (3%)
10. Poland (3%)

INTERNATIONAL ASPECTS OF CYBER LAWS

The advancement of internet has enabled users to access information which was a dream once, and the technology like Voice over Internet Protocol (VoIP) has revolutionized communication. One can access information without suffering barriers available in internet, no matter whether which country hosts it.

A specialized agency of the United Nations, responsible for issues concerning information and communication technologies is International Telecommunications Union. Information and communication streaming around the world is swift and smooth as never before. Although, physical border still has importance, but ones and zeros, bits and bytes flow with a continual change of places among countries freely. Cyber criminals avail this advantage and commit crimes on places other than where they are located. National supremacy is no more an issue for the transnational cybercrime.

The significance of respective issue made developing countries more concerned to cautiously build and deploy the security and trust. So, the benefits and advantages of ICTs can serve their citizen not only for commercial activities, but its application can be make useful at societal level such as health, education, and e-government, etc. International aspects of cyber laws encompasses:

1. To identify cybercrime threats and vulnerabilities and deploy solutions to secure ICT infrastructure for internet consumers and its application on different networks using pertinent technologies.
2. To support and work along with member states in gradual developments of laws and set exemplary legislation for internet services, internet security, its ethical issues, deterrence of cybercrime, data security, as well as privacy.
3. To increase security and make cyber environment as unattractive as possible to cyber criminal, so that confidence of consumer is enhance while using internet services and respective applications.
4. To develop hardware and software tools to promote and exchange best possible practices on ICTs security and related legitimate concerns in the respective areas.

INITIATIVES BY THE EU AND USA

The initiatives regarding cyber law by the United States of America are discussed below because of the role of USA as a global superpower in terms of technology and world's strongest economy in terms of nominal GDP, i.e. \$20.891 trillion (IMF, 2018). While, the European Union is a political and economic union of 28 member states, and accounts for being the strongest monetary union in the world with a nominal GDP \$19.14 trillion (ibid.). People's Republic of China is the third largest economy of the world after the US and the EU. It boosts for being a regional superpower as it has a nominal GDP of \$14.21 trillion (ibid.).

In almost all European countries, the European Union has implemented the rules and regulation on electronic trade and commerce through legislation and makes sure that non-member countries align their laws with the EU initiative.

USA's experience and knowledge in the field of legislation regarding cyber security is significant. The USA has organized and featured structure for consumers of ICT to report cybercrime against them. The foremost federal law enforcement agencies which are responsible for investigation of cybercrime at domestic level include:

1. United States Secret Service (USSS)
2. Federal Bureau of Investigation (FBI)
3. United States Postal Inspection Service (USPIS)
4. United States Immigration and Customs Enforcement (ICE)
5. Bureau of Alcohol, Tobacco and Firearms (ATF)

In almost all European countries, the European Union has implemented the rules and regulation on electronic trade and commerce through legislation and makes sure that non-member countries align their laws with the EU initiative.

USA's experience and knowledge in the field of legislation regarding cyber security is significant. The USA has organized and featured structure for consumers of ICT to report cybercrime against them. The foremost federal law enforcement agencies which are responsible for investigation of cybercrime at domestic level include:

Every state has offices for cybercrime monitoring agencies where crime can be reported conveniently. Every state office has a predefined contact information which is easy to access and cybercrime can be reported to the local office of concerned agency by even a phone call to an available duty complaint officer.

Every law enforcement agency headquarters are situated in Washington, D.C, where a number of law enforcing officers who are well trained and specialized in their particular fields are working vigilantly. Federal Bureau of Investigation and USA Secret Service, both have their head offices in Washington and are responsible for protecting forcible intrusion by cyber criminals. For most of the time, the aim of cyber criminals is either monetary gains or access to classified data. Generally, they are termed as hackers, i.e., they hack into legitimate computer networks.

Federal Bureau of Investigation in collaboration with National White Crime Complaint Centre, another US prominent agency, established Internet Crime Complaint Centre (IC3) in 2000. It is serving as a platform to receive cybercrime complaints, develop strategies, and refer cybercrime complaints to confront increasing cyber threats.

The IC3 has remarkably a positive staff culture regarding cybercrime victims where one can report crime because of their friendly reporting system which immediately make sure that concerned authori-

ties are notified and appropriate action against cyber criminal has been initiated. IC3 also makes sure that the central referral mechanism is intact for regulatory and law enforcement agencies at the federal, state, and local level.

Other Initiatives by the Government of United States Regarding Cybercrime

1. Online Copyright Infringement Liability Limitation Act - 1998
2. Digital Millennium Copyright Act - 1998
3. Uniform Computer Information Transactions Act - 1999
4. Internet Fraud Complaint Center (IFCC) (founded in 2000)
5. U.S. Computer Emergency Readiness Team (founded in 2003)
6. Controlling the Assault of Non-Solicited Pornography And Marketing Act - 2003
7. Proposed EU Directives on the patentability of computer-implemented inventions.
8. National Association of Attorney General's Computer Crime Point of Contact List.
9. Department of Homeland Security's National Infrastructure Coordinating Center.

INITIATIVES BY CHINA

The second largest internet users after USA are from the People's Republic of China. There are approximately 111 million internet users in this country. China reaps the advantages of technological growth, but at the same time while such a huge number of people were accessing internet, regulation as well as supervision from authorities were lacking. It caused a rampant growth in cybercrime, which include the spread of pornographic material, hate and harm content, illicit gambling, online frauds, etc.

Chinese authorities addressed the issues exemplary. They deployed surveillance and regulated their internet users, which not only mitigated the growth of cybercrime, but also left a positive growth on their e-trade.

Shenzhen, in southeastern China, is a modern metropolis, according to the statistics presented by the Shenzhen Association of Online Media and the China Internet Network Information Center (CINIC), there were 8.97 million internet users in Shenzhen by the end of 2015. The highest ratio nationwide, which is 83.2 percent of Shenzhen's total population, is on top of achieving success regarding online crimes and rapid spread of malicious and hazardous information by forming a cyber police force.

Cyber police in China has developed a system to patrol and keep active presence on online activities of users. When a user gets online, an icon which shows the presence of police department flashes on the user's screen. Whenever a user needs to contact for a cybercrime complain, he just has to click the respective icon, and can report to the immediate complaint officer in few minutes.

In a few months time, cyber police has been notified regarding online crimes by clicking icon that accumulated around 100,000 clicks, which include more than 600 consultation services on cybercrime legislation along with 1,600 reports of online criminal activities, out of which 235 have been forwarded for legal proceedings. The Ministry of Public Security has decided to establish cyber police in eight major cities of China after the success in Shenzhen.

Role of Chinese Cyber Police

1. Cyber police vigilantly patrol online, where cybercrime ratio is high to warn cyber criminals.
2. Internet users can easily access information regarding cyber legislation and understanding of complication of cyber criminal cases.
3. The cyber police force not only records the complain regarding cybercrime, but also assists online users about legal aspects concerning cybercrime.

INTERNATIONAL FORUM FOR CYBERCRIME

The invention of internet has created many possibilities and opportunities for artistic and literary creation. Although, we find traditional laws of copyright in physical world, but legislation for cyberworld in other domains is necessary and of immense importance. World Intellectual Property Organization (WIPO) addressed the respective issue via two treaties, i.e.,

1. World Intellectual Property Organization Copyright Treaty of 1996
2. World Intellectual Property Organization Performances and Phonograms Treaty of 1996

These treaties are implemented in the European Union, USA, Canada, as well as other nation states.

An agreement between member countries of European Union (EU) in 2001 regarding cybercrime is considered to be the first international initiative on computer crime. It is referred to as the Council of Europe - Convention on Cybercrime 2001. It has been implemented in July 2004 and signed by 37 countries.

It is a great effort which aids in the advancement of international cooperation through legislation of conventional cybercrime. It provides the basic framework and common legislative grounds to member countries, instead of their national laws for cybercrime. It is indeed, a landmark to prosecute cyber criminals, who commit crime in one country, but have an adverse effect on other countries.

Cyber security has become a global issue which undoubtedly demand a global approach for prevention of real time borderless exchange of classified and non-classified data by cyber criminals which are mostly attained through hacking.

The United Nations Congress on Crime Prevention and Criminal Justice emphasized on member states to develop an organized and international response to the misuse of ICTs. UN developed some guidelines and principles for the states to elaborate the legislation process. While, the implementation of such legislation are state's responsibility.

The United Nation Resolution 55/56 and 56/121 are an attempt to fight against the illegitimate use of ICTs and elimination of safe haven by requesting member states to incorporate effective legislation for the removal of such safe havens from their territory. Resolutions 57/239 and 58/199 addresses the need of awareness, adopting a global security culture, as well as protection of ICTs infrastructure from criminals.

The Organisation for Economic Co-operation and Development is an intergovernmental economic organization with 36 member countries, established in 1961. OECD replaced it guidelines published in 1992 regarding security policies with the Guidelines for the Security of Information Systems and Network 2002.

It provides a framework to member countries that support them in establishing the security for their interconnected communications systems and networks, along with the adaptation of security culture among users.

SOLUTIONS AND RECOMMENDATIONS

1. A strong global cyber force is required who can counter cyber threats.
2. Proper cybercrime data should be maintained by respective countries and it should be shared to the possible extent.
3. Victims of cybercrime are large in number, there should be easy access of the victims where they can complain regarding e-offenses.
4. Private companies should develop the liaison with the government officials to maintain the swiftness of their internet approach.
5. The respective legal departments should be equipped with the latest investigating technologies.

FUTURE RESEARCH DIRECTIONS

The significant areas for conducting future research encompassing cybercrime via engaging qualitative, qualitative, or eclectic approach can be:

1. Cybercrime and freedom of speech.
2. Low conviction rates of cyber criminals.
3. Cyberterrorism and cyber violence.
4. Cyber security issues.

CONCLUSION

In the contemporary era, the internet is indeed a very compelling invention, as it influence almost everyone who uses it. Research studies encompassing cybercrime are nominal as compared to conventional crimes. People who are more dependent on technology, become easy targets of cybercrime across the globe.

Nations worldwide are facing the hazards of cybercrime, because of numerous causes, poor technology, lack of cooperation with international law enforcing agencies, and absence as well as incapacity of legislation to financial constraints. Thus, solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments.

Comprehensive cyber laws in an international context are a dire need of time. Furthermore, cyber laws have been developed in almost every developing as well as developed country, but their implementation is comparatively weak.

REFERENCES

- Alvarez Technology Group. (2018). *2018 Top Cybercrime Facts and Why You Should Care*. Retrieved May 11, 2019, from <https://www.alvareztg.com/2018-cybercrime-statistics-reference-material/>
- Bischoff, P. (2018, September 6). *Analysis: How data breaches affect stock market share prices*. Retrieved August 19, 2018, from <https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/>
- Brenner, S. W. (2014). *Cyberthreats and the decline of the nation-state*. Routledge. doi:10.4324/9780203709207
- Bromium, & McGuire, M. (2018, April). *RSA Conference 2018*. Retrieved July 19, 2018, from <https://www.rsaconference.com/events/us18>
- Council of Europe - Convention on Cybercrime. (2001). Retrieved July 19, 2018, from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest/7_conv_budapest_en.pdf
- Cybersecurity Ventures. (2017). *Cybercrime Report*. Retrieved September 29, 2018, from <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- Ekblom, P. (2014). Designing products against crime. In *Encyclopedia of Criminology and Criminal Justice* (pp. 948–957). Springer. doi:10.1007/978-1-4614-5690-2_551
- Glenny, M. (2012). *DarkMarket: How hackers became the new media*. Vintage Books.
- Hutchings, A. (2013). *Theory and crime: Does it compute?* Griffith University.
- International Monetary Fund. (2018). *World Economic Outlook Database*. Retrieved May 15, 2019, from <https://www.imf.org/external/pubs/ft/weo/2018/02/weodata/weorept.aspx?pr.x=42&pr.y=2&sy=2019&ey=2023&scsm=1&ssd=1&sort=country&ds=.&br=1&c=998&s=NGDPD%2CPPPGDP%2CPPPPC&grp=1&a=1>
- Jones, C. W. (2005, April). *Council of Europe Convention on Cybercrime: Themes and critiques*. Workshop on the International Dimensions of Cyber Security. Hosted by Georgia Institute of Technology and Carnegie Mellon University.
- Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, 13(2), 71–94. doi:10.1080/17440572.2012.674183
- Milkovich, D. (2018, December 3). *13 Alarming Cyber Security Facts and Stats*. Retrieved May 12, 2019, from <https://www.cybintsolutions.com/cyber-security-facts-stats/>
- NC Report. (2011). Retrieved March 11, 2018, from http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/
- Nohe, P. (2018, September 27). *Re-Hashed: 2018 Cybercrime Statistics: A closer look at the Web of Profit*. Retrieved May 12, 2019, from <https://www.thesslstore.com/blog/2018-cybercrime-statistics/>
- Ponemon Institute. (2018). *State of Endpoint Security Risk*. Retrieved September 17, 2018, from <https://www.businesswire.com/news/home/20181016005758/en/Study-Reveals64-Organizations-Experienced-Successful-Endpoint>

Sandwell, B. (2010). On the globalisation of crime: The internet and new criminality. In Y. Jewkes & M. Yar (Eds.), *Handbook of internet crime* (pp. 38–66). Uffculme, UK: Willan Publishing.

Shenzhen Association of Online Media and China Internet Network Information Center. (2015). Retrieved June 29, 2018, from http://english.sz.gov.cn/ln/201601/t20160121_3452230.htm

Smith. (2018). *Hacking pacemakers, insulin pumps and patients' vital signs in real time*. Retrieved September 10, 2018, from <https://www.csoonline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html>

Summo3000. (2018). *Top 20 Countries Found to Have the Most Cybercrime*. Retrieved May 12, 2019, from <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>

Symantec White Paper - Turning the Tables on Malware. (2012). Retrieved June 22, 2018, from https://www.symantec.com/content/en/us/enterprise/white_papers/b-turning_the_tables_on_malware_WP_21155056.en-us.pdf

Yar, M. (2013). *Cybercrime and society*. London: Sage Publishing Ltd.

ADDITIONAL READING

Bandura, A. (2007). Impeding ecological sustainability through selective moral disengagement. *International Journal of Innovation and Sustainable Development*, 2(1), 8–35. doi:10.1504/IJISD.2007.016056

Broadhurst, R., & Choo, K. K. R. (2011). *Cybercrime and online safety in cyberspace*. Routledge Handbook of Criminology.

Clarke, R. V. (2012). Opportunity makes the thief. Really? And so what? *Crime Science*, 1(1).

Cloward, R., & Ohlin, L. (2013). *Delinquency and opportunity: A study of delinquent gangs*. Routledge. doi:10.4324/9781315007274

Cornish, D. B., & Clarke, R. V. (Eds.). (2014). *The reasoning criminal: Rational choice perspectives on offending*. Transaction Publishers.

Downes, D. M., & Rock, P. (2011). *Understanding deviance: A guide to the sociology of crime and rule-breaking*. Oxford, UK: Oxford University Press. doi:10.1093/he/9780199569830.001.0001

Hagan, F. E. (2012). *Introduction to criminology: Theories, methods, and criminal behavior*. Los Angeles, CA: Sage.

Hirschi, T. (1969). *Causes of delinquency*. Berkeley, CA: University of California Press.

Isajiw, W. W. (2013). *Causation and functionalism in sociology*. Routledge. doi:10.4324/9781315888699

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4), 757–780. doi:10.1111/1467-954X.00139

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in Organized Crime*, 17(4), 231–249.

Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *Security & Privacy*, 11(1), 78–81.

Urbas, G., & Choo, K. R. (2008). *Resource materials on technology-enabled crime*. Canberra, Australia: Australian Institute of Criminology.

Wall, D. S. (Ed.). (2001). *Crime and the internet*. New York: Routledge. doi:10.4324/9780203164501

Yar, M. (2013). *Cybercrime and society*. London: Sage Publishing Ltd.

KEY TERMS AND DEFINITIONS

Cyber Security: Security on the internet.

Cybercrime: The use of a computer to commit a crime.

Cybercrime Legislation: The process of making laws regulating cybercrime.

Cyberterrorism: The use of information and communication technology to cause grave disruption or pervasive fear.

Cyberworld: The world of inter-computer communication.

International Cooperation and Legal Response to Cybercrime in Pakistan

Tansif Ur Rehman

University of Karachi, Pakistan

INTRODUCTION

According to Internet World Stats (IWS), the total number of internet users in Pakistan during October 2018 were 44,608,065, which is 22.2% of the total population. More than 30 million of Pakistan's 212 million people use the internet via mobile devices (Bytes for All, 2017). The literacy rate of the country is quite low as compared to other countries, i.e., 58 percent (Economic Survey of Pakistan, 2017).

Research studies into cybercrime with regards to the Pakistani context are nominal, as the field is relatively new. Pakistani has a perfect ecosystem regarding cybercrime, as the internet is widely available. Laws regarding cybercrime exist in Pakistan, but are rarely enforced. The respective culprits usually go largely unpunished in Pakistan. Most common types of cybercrime in Pakistan are criminal access, e-fraud and e-forgery, misuse of devices and encryption, cyberstalking, pornography, malicious code, spamming, unauthorized interception, cyberterrorism, attempt and aiding or abetting.

This research focuses on the common patterns of cyber criminals and the required legislation and enforcement of existing laws along with the need of international cooperation to counter global cyber threat.

OBJECTIVES

1. To highlight the main aims of Electronic Transactions Ordinance, 2002.
2. To highlight the formation of National Response Centre for Cyber Crime.
3. To critically analyze the role of Prevention of Electronic Crimes Act, 2016.
4. To highlight the legislation in Pakistan for international cooperation regarding cybercrime.
5. To discuss the legal response to cybercrime in Pakistan.

BACKGROUND

A bill has to be passed by both Houses of Parliament, i.e. the National Assembly and the Senate. Upon a bill's passage through both Houses, it is presented to the President of Pakistan for assent and becomes an Act of Parliament upon receiving such assent. In National Assembly's absence, statutes are promulgated by the President. The President may, if satisfied that circumstances exist which render it necessary to take immediate action, make and promulgate an Ordinance (Sial & Iqbal, 2015).

The respective framework, i.e., Electronic Transactions' Ordinance, 2002 has provided Pakistan with an initial legal backing regarding e-information as well as communication. National Response Centre for Cyber Crime (NR3C) formed in 2007 is another initiative taken by the Government of Pakistan to trace cyber criminals and to counter the internet misuse.

DOI: 10.4018/978-1-5225-9715-5.ch029

While, the National Assembly of Pakistan has passed the draft of Prevention of Electronic Crimes Act, 2016 (PECA) on 13th April, 2016 after making various amendments to it. PECA was drafted as being part of the National Action Plan (NAP), which was developed in response to the December 2014 attack on Army Public School, Peshawar. This attack took life of 150 people (including 132 children) (Khan, 2018). NAP is a 20 points plan for countering terrorism as well as extremism. It was drafted by the National Counter Terrorism Authority and Ministry of Interior. It got approval from the Parliament on December 24, 2014 (Haider, 2014).

Anusha Rahman Khan - Minister of State for Information Technology and Telecommunication of Pakistan and member of the committee for development of 'Prevention of Electronic Crimes Act, 2016' (PECA) admitted in a summarized note that, Pakistan has no such laws before to deal comprehensively with cybercrime. She belongs to Pakistan Muslim League (Nawaz), which is a centre-right conservative party in Pakistan. She also admitted that, criminal justice legal framework is ill equipped as well as inadequate and to resolve the respective threats of the cyber age.

Although, the PECA has been approved and came into system, but there is huge criticism from the opposition and the IT industry. Critics believe it to be harsh, with punishments not fitting the respective crimes. Another problem is the bill's language, as it could be abused by the government as well as law enforcement agencies in Pakistan.

FOCUS OF THE ARTICLE

This article focuses on the role of Prevention of Electronic Crimes Act (2016), legislation in Pakistan for international cooperation regarding cybercrime, as well as the legal response to cybercrime in Pakistan. This research also cites almost all relevant laws relevant to cybercrime, which have been legislated by the governmental body and defines what is illegal in the Pakistani context. This will help to understand the computer-related crime advancement, and how to use it as defined within the premises of law in the Pakistani context.

ELECTRONIC TRANSACTIONS ORDINANCE, 2002

The implementation of Electronic Transactions Ordinance, 2002 (ETO) has placed Pakistan in those few countries who understood the importance of cybercrime legislation in early time and provided imperative guidelines and frameworks which enabled and encourage the IT industry to foster at higher standards and spread of e-commerce in Pakistan. The Electronic Transaction Ordinance is of high importance that is necessary in carrying out proper IT growth and considered as a turning point for the Information and Communication Technology development as well as growth in Pakistani context.

Ordinance's Main Aim

1. Enhanced electronic transactions.
2. Legal and safe trading platforms for sellers as well as buyers.
3. Economic upheaval.
4. Growth in e-commerce and projection of surgical items, sports goods, leather goods, as well as textile products in the international market.

5. Enhanced punishments for offenses involving sensitive electronic systems.
6. Cost reduction strategies for small and medium business enterprises via e-transactions.

Main Clauses Cover Enlisted Offenses

1. Unauthorized interception
2. Spamming
3. Malicious code
4. Misuse of devices
5. Electronic fraud
6. Data damage
7. Criminal access
8. Issue of false certificate
9. Cyber terrorism
10. Spoofing
11. Cyberstalking
12. Misuse of encryption
13. Electronic forgery
14. System damage
15. Criminal data access
16. Damage to information system
17. Attempt and aiding or abetting
18. Provision of false information
19. Waging cyber war

NATIONAL RESPONSE CENTRE FOR CYBER CRIME

National Response Centre for Cyber Crime (NR3C) formed in 2007 is another initiative taken by the Government of Pakistan to trace cyber criminals and to counter the internet misuse. Regarding the 'Certificate Authority (CA)', the Ministry of Information Technology and Telecommunication (MoITT) formed the Accreditation Council in accordance with the National IT Policy and Electronic Transactions Ordinance, 2002.

This voluntary licensing program aims at promoting high integrity licensed CAs that can be trusted. A Certificate Authority aiming to acquire a license will adhere to a more stringent licensing criteria, which includes:

1. Strict security procedures as well as controls
2. Personnel integrity
3. Financial soundness

PREVENTION OF ELECTRONIC CRIMES ACT, 2016

The National Assembly of Pakistan has passed the draft of Prevention of Electronic Crimes Act, 2016 (PECA) on 13th April, 2016. One of the principal reason for drafting the respective Act was to provide a legal framework for attack against computers. Section 3 to 8 of this Act set out enlisted provisions.

1. Unauthorized access to data or Information System (IS).
2. Unauthorized transmission or copying of data.
3. Interference with data or Information System (IS).
4. Unauthorized access to data or Critical Infrastructure Information System (CIIS).
5. Unauthorized transmission or copying of Critical Infrastructure Data (CID).
6. Interference with data or Critical Information System (CIS).

LEGISLATION IN PAKISTAN FOR INTERNATIONAL COOPERATION

Chapter 4, Article 42, of the Prevention of Electronic Crimes Act, 2016 in this context states that;

1. The Federal government may upon receipt of a request, through the designated agency under this Act, extend such cooperation to any foreign government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offenses related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offense or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act.
2. The Federal Government may forward to a foreign government, 24x7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offense under this Act.
3. The Federal Government shall require the foreign government, 24 x 7 network any foreign agency or any international organization or agency to keep the information provided confidential and use it strictly for the purposes it is provided.
4. The Federal Government may, through the designated agency, send and answer requests for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution.
5. The Federal Government may refuse to accede to any request made by a foreign government 24 x 7 network any foreign agency or any international organization or agency, if
 - a. It is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interest of Pakistan;
 - b. The offense is regarded by the Federal Government as being of a political nature
 - c. There are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that persons race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons;

- d. The request relates to an offense the prosecution of which in the requesting State may be incompatible with the laws of Pakistan;
 - e. The assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offense been the subject of investigation or prosecution under its own jurisdiction; or
 - f. The request concerns an offense which may prejudice an ongoing investigation or trial or rights of its citizens guaranteed under the Constitution.
6. Where the Federal Government decides to provide the requested cooperation, the relevant requirements and safeguards provided under this Act and rules framed thereunder shall be followed.
7. The designated agency shall maintain a register of requests received from any foreign government,²⁴ x 7 network, any foreign agency or any international organization or agency under this act and action taken thereon.

LEGAL RESPONSE TO CYBERCRIME IN PAKISTAN

Legal Response to Cyberterrorism in Pakistan

Regarding cyberterrorism Prevention of Electronic Crimes Act, 2016, article 10 and 12 of chapter two states;

“Whoever commits or threatens to commit any of the offenses under sections 6, 7, 8 or 9, where the commission or threat is with the intent to;

- a. Coerce, intimidate. create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of[lear or insecurity in society: or
- b. advance inter-faith, sectarian or ethnic hatred; or advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend for fourteen years or with fine which may extend to fifty million rupees or with both.
- c. Recruitment, funding and planning of terrorism. Whoever prepares or disseminates information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plan for terrorism shall be punished with imprisonment for a term which may extend to seven years or with fine or with both”.

Legal Response to Fraud in Pakistan

Regarding Cyber Fraud (PECA) in article 14, 23, 25, and 26 of chapter two (2) states:

Article 14 (Electronic Fraud):

Whoever with the internet for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.

Article 23 (Malicious Code):

Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction alteration, suppression, then or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or with both.

Article 25 (Spamming):

1. A person commits the offense of spamming, who with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain.
2. A person including an institution or an organization engaged in direct mailing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing.
3. Whoever commits the offense of spamming as described in sub-section (1) by transmitting harmful, fraudulent, misleading or illegal information, shall be furnished with imprisonment for a term which may extend to three months or with fine of rupees fifty thousand which may extend up to rupees five million or with both.
4. Whoever commits the offense of spamming as described in sub-section by transmitting unsolicited information, or engages in direct marketing in violation of sub-section for the first time, shall be punished with fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with fine not less than fifty thousand rupees that may extend up to one million rupees.

Article 26 (Spoofing):

Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing

Legal Response to Hate Crime in Pakistan

Regarding Hate crime (PECA) in article 11 of chapter two (2) states;

Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

Legal Response to Sexualized Content in Pakistan

Regarding sexualized content (PECA) in article 21 and 23 of chapter two states:

1. Whoever intentionally and publicly exhibits or displays or transmits any information which,
 - a. Superimposes a photograph of the face of a natural person over any sexually explicit image or video, or

- b. Includes a photograph or a video of a natural person in sexually explicit conduct; or
 - c. Intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person;
 - d. Cultivate, entices or induces a natural person to engage in a sexually explicit act,
 - e. Through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both.
2. Whoever commits an offense under sub-section (1) with respect to a minor shall be punished with imprisonment for a term which may extend to seven years and with fine which may extend to five million rupees: Provided that in case of a person who has been previously convicted of an offense under sub-section (1) with respect to a minor shall be punished with imprisonment for a term of ten years and with fine.
3. Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

Legal Response to Child Pornography in Pakistan

1. Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in the information system that visually depicts
- a. A minor engaged in sexually explicit conduct
 - b. A person appearing to be a minor engaged in sexually explicit conduct or
 - c. Realistic images representing a minor engaged in sexually explicit conduct or
 - d. Discloses the identity of the minor,

shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both”.

2. Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

Legal Response to Cyberstalking in Pakistan

Regarding Cyberstalking (PECA) in article 24 of chapter two (2) states that

1. A person commits the offense of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the internet, website, electronic mail or any other similar means of communication to
 - a. Follow a person or contacts or attempts to contact such person to foster personal information repeatedly despite a clear indication of disinterest by such person
 - b. Monitor the use by a person of the internet, electronic mail, text message or; my other form of electronic communication;
 - c. Watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or
 - d. Take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person.
2. Whoever commits the offense specified in sub-section (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both: Provided that victim of the cyber stalking under sub-section
 - a. Is a minor the punishment may extend to five years or with fine which may extend to ten million rupees or with both.
3. Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

CRITICISM OF PECA

Prevention of Electronic Crimes Act, 2016 is also facing harsh criticism from different political groups, religious groups, INGOs, NGOs, as well as CBOs. According to them, punishment lacks the relevancy to crime, and there are also many ambiguities in the respective act which may cause suffering to users by law enforcers in Pakistan (Jahangir, 2018; Khan, 2016).

ICTs organizations and cybercrime specialist were not taken on-board during the preparation of the act. It is also said that restrictions have been imposed on freedom of expression and access to available information on cyberworld. As cybercrime has a relation to the physical world, many articles in this act are overlapping with previously existing laws. Critics feel that this act can be misused against journalists as well as whistle blowers.

The surveillance criteria does not match the existing act of Fair Trial 2013. How law enforcing agencies will make its implementation possible, while the criminal trial procedure is unclear.

Although critics are claiming that cyberterrorism is not the subject of the bill, therefore terrorism clauses should be removed. While, the world perceives cyberterrorism as the most dangerous threat from intruders. According to a leading United States' newspaper report, i.e., New York Times by David E. Sanger and William Broad (2018), the USA government is even considering the use of nuclear weapon in the fight against cybercrime.

It is unclear how Pakistani authorities will block or remove online material, and which material will be considered illicit, will law enforcers need court orders to remove online material? Critics are having

difficulties in differentiating cyberterrorism and cyberwarfare, that whether it is a category of cybercrime or has some other definite form in the context of Pakistan.

SOLUTIONS AND RECOMMENDATIONS

1. General public awareness programs should be initiated with regards to cybercrime in Pakistan.
2. During the process of legislation regarding cybercrime in Pakistan, expert opinion should be included, like criminologists, psychologists, sociologists, IT professionals, etc.
3. Pakistan should maintain proper cybercrime data.
4. Victims of cybercrime are large in number, there should be easy access of the victims where they can complain regarding e-offenses.
5. Private companies should develop a strong liaison with the Government of Pakistan regarding the swiftness of their internet approach.
6. Pakistani legal department should be equipped with the latest investigating technologies.
7. Pakistani scholars should discuss cybercrime issue on different forums, specially in print as well as electronic media.
8. To effectively deal with cases of cybercrime, the respective judiciary must be given proper training.

FUTURE RESEARCH DIRECTIONS

The significant areas for conducting future research encompassing cybercrime via engaging qualitative, qualitative, or eclectic approach can be:

1. Cybercrime and freedom of speech in Pakistan.
2. Low conviction rates of cyber criminals in Pakistan.
3. Cyberterrorism and cyber violence in Pakistan.
4. Cyber security issues in Pakistan.

CONCLUSION

For developing countries, like Pakistan to trade with the developed ones, they must ensure that their national legislation ensures the same level of protection granted by other countries regarding storage and processing of personal data. This is imperative if these countries want to trade with European Union countries, which possess a very strong data protection laws.

The Federal Investigation Agency (FIA) of Pakistan was allowed by the Ministry of Interior to establish 15 cybercrime reporting centres across the country in October 2018 (Azeem, 2018). According to the FIA Cybercrime Director Captain Mohammad Shoaib (June 2018) statement, in the last three years, cybercrime has increased sharply in Pakistan. He further shared with the Standing Committee - Senate of Pakistan that, the Federal Investigation Agency has 10 experts only to investigate cybercrime (Qarar, 2018).

REFERENCES

- Azeem, M. (2018, October 03). FIA allowed to open 15 centres to check cybercrime. *Dawn*. Retrieved from <https://www.dawn.com/news/1436438>
- Government of Pakistan. (n.d.). *Investigation for Fair Trial Act, 2013*. Retrieved from http://www.na.gov.pk/uploads/documents/1361943916_947.pdf
- Government of Pakistan Bureau of Statistics. (2018). *Provisional Summary Results of 6th Population and Housing Census - 2017*. Retrieved from <https://bytesforall.pk/>
- Government of Pakistan. (2018). *National Response Centre for Cyber Crime*. Retrieved from <http://www.nr3c.gov.pk/cybercrime.html>
- Government of Pakistan. Ministry of Finance, Revenue & Economic Affairs. (2018). *Economic Survey of Pakistan, 2017*. Retrieved from http://www.finance.gov.pk/survey_1617.html
- Government of Pakistan. Ministry of Information Technology and Telecommunication. (2018). *Electronic Transactions Ordinance, 2002*. Retrieved from <http://www.pakistanlaw.com/eto.pdf>
- Government of Pakistan. Ministry of Information Technology and Telecommunication. (2018). *Prevention of Electronic Crimes Act, 2016*. Retrieved from http://www.na.gov.pk/uploads/documents/1470910659_707.pdf
- Haider, M. (2014, December 24). Political leaders reach consensus on military courts. *Dawn*. Retrieved from <https://www.dawn.com/news/1152909/political-leaders-reach-consensus-on-military-courts>
- Internet World Stats. (2018). Retrieved from <https://www.internetworldstats.com/asia/pk.htm>
- Jahangir, R. (2018, October 28). Pakistan's online clampdown. *Dawn*. Retrieved from <https://www.dawn.com/news/1441927>
- Khan, E. A. (2018). The Prevention of Electronic Crimes Act 2016: An analysis. *LUMS Law Journal*, 5. Retrieved from <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis>
- Khan, R. (2016, April 13). Controversial cyber crime bill approved by NA. *Dawn*. Retrieved from <https://www.dawn.com/news/1251853>
- Qarar, S. (2018, October 23). Cybercrime reports hit a record high in 2018: FIA. *Dawn*. Retrieved from <https://www.dawn.com/news/1440854>
- Sanger, D. E., & Broad, W. (2018, Jan 16). Pentagon suggests countering devastating cyberattacks with nuclear arms. *New York Times*. Retrieved from <https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html>
- Sial, O., & Iqbal, S. (2015, November). *A Legal research guide to Pakistan*. Retrieved from <https://www.nyulawglobal.org/globalex/Pakistan.html>

ADDITIONAL READING

- Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: Trends and challenges. In *Handbook of Asian criminology* (pp. 49–63). New York: Springer. doi:10.1007/978-1-4614-5218-8_4
- Clarke, R. V. (2012). Opportunity makes the thief. Really? And so what? *Crime Science*, 1(1).
- Imam, A. L. (2012 December). *Cyber crime in Pakistan: Serious threat but no laws!* Retrieved from <http://blogs.tribune.com.pk/story/15063/cyber-crime-in-pakistan-serious-threat-but-no-laws/>
- Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in Organized Crime*, 17(4), 231–249.
- Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, 13(2), 71–94. doi:10.1080/17440572.2012.674183
- Mohiuddin, Z. (2006 June). *Cyber laws in Pakistan: A situational analysis and way*. Retrieved from <http://www.supremecourt.gov.pk/ijc/articles/10/5.pdf>
- Momein, F. A., & Brohi, M. N. (2010). Cybercrime and internet growth in Pakistan. *Asian Journal of Information Technology*, 9(1), 1–4. doi:10.3923/ajit.2010.1.4

KEY TERMS AND DEFINITIONS

Cyber Security: Security on the internet.

Cybercrime: The use of a computer to commit a crime.

Cybercrime Legislation: The process of making laws regulating cybercrime.

Cyberstalking: The use of information and communication technology to frighten or harass an individual or group.

Cyberterrorism: The use of information and communication technology to cause grave disruption or pervasive fear.

Cybersecurity Laws in Malaysia

2

Olivia Swee Leng Tan <https://orcid.org/0000-0002-5628-6883>*Multimedia University, Malaysia***Rossanne Gale Vergara***Multimedia University, Malaysia***Raphael C. W. Phan***Multimedia University, Malaysia***Shereen Khan***Multimedia University, Malaysia***Nasreen Khan***Multimedia University, Malaysia*

INTRODUCTION

The progression of information and communication technologies (ICT) use have been matched by the rise in corruption and abuse of technology for criminal activities. Regarding computer crimes in Malaysia, the Malaysia Computer Emergency Response Team (MyCERT) reported 3,743 incidents from January to May of 2019. Fraud incidents at 2,563 ranking the highest reported incidents for 2019 and “intrusion” incidents at 432 ranking the second highest incidents. In 2018, the total incidents reported to MyCERT was 10,699, of which “fraud” again had the highest reported incidents (5,123) and the second highest “intrusion attempt” at (1,805) of the total incidents. Between 2014-2017, the total number of incidents (Cyber harassment, Content related, Denial of Service, Fraud, Intrusion, Intrusion Attempt, Malicious Codes, Spam, Vulnerabilities report) gradually decreased from 11,918 incidents in 2014 to 7,962 incidents, a decrease of 3,956 or 33.2% in 2017. The statistics show that Malaysia’s cybercrime incidents have increased again in 2018 despite the country’s attempts at mitigating cybercrime. Cybercrimes are borderless and the threat of a cyberattack or cybercrime is there. To combat such criminal activities today in Malaysia, cyber laws have existed since 1997 to include: Computer Crimes Act 1997, Digital Signature Act 1997, Communications and Multimedia Act 1998, Payment Systems Act 2003, Electronic Commerce Act 2006, Personal Data Protection Act 2010 and Malaysian Penal Code to combat criminal activities such as fraud. While the cyber laws and law enforcement agencies exist in Malaysia, cybercrimes still pose a daunting challenge. The objective of this chapter is to analyse the existing cyber security legislations in Malaysia to combat cybercrimes in the country.

DOI: 10.4018/978-1-5225-9715-5.ch030

BACKGROUND

In 1991, Malaysia Vision 2020 by Prime Minister Mahathir Mohamad was presented during the Sixth Malaysia Plan. Malaysia Vision 2020 was the prime minister's vision for Malaysia to become a developed nation by 2020, which included his thoughts on how the nation can achieve this goal by meeting nine specific objectives. These nine objectives as he pointed out in his vision were to establish the following:

1. United Malaysian nation
2. Secure and developed Malaysian Society
3. Mature democratic society
4. Fully moral and ethical society
5. Matured liberal and tolerant society
6. Scientific and progressive society, a society that is innovative and forward looking, one that is not only a consumer of technology but also a contributor to the scientific and technological civilisation of the future
7. Fully caring society and caring culture
8. Economically just society
9. Prosperous society, with an economy that is fully competitive, dynamic, robust and resilient.

Malaysia Vision 2020 catapulted initiatives to support Prime Minister Mahathir's agenda, one of these listed as objective six: to establish a scientific and progressive society. Thus, Multimedia Super Corridor (MSC) Malaysia was launched in 1996 and the first cyber laws of Malaysia were introduced: Computer Crimes Act 1997, Telemedicine Act 1997, Copyright (Amendment) Act 1997, and Digital Signature Act 1997. Communication and Multimedia Act 1998 followed one year later and then: Payment Systems Act 2003, Electronic Commerce Act 2006, and Personal Data Protection Act 2010. The foundation established by these early cyber laws were to prepare the nation to embark on innovations and protect Malaysians using new innovations. The laws most relevant to current cybercrimes experienced in Malaysia will be discussed further in the subsequent section.

Malaysia, a country with a population of 32.7 million located in Southeast Asia was ranked third overall in the world behind Singapore and United States in the 2017 Global Cyber security Index (GCI), (International Telecommunications Union, 2017, July 6) and currently 8th place in the 2018 GCI global ranking. GCI is a survey that measures the commitment of the International Telecommunications Union (ITU) Member States to cyber security in order to raise awareness, which is driven by five pillars (legal, organisational, capacity building, and cooperation). However, as mentioned above, while the incidents reported by MyCERT have decreased from 2014-2017, the reported incidents have increased since then by 2,737 incidents in 2018. Table 1 below shows the top five reported incident categories (Fraud, Intrusion, Intrusion Attempt, Spam, Malicious Code) by MyCERT from 2010-2018, with the exception of "Cyber Harassment" making it to the top 5 incidents in 2018 overtaking Spam incidents. 2011 was the year Malaysia had the highest overall reported incidents in fraud (5,328) and spam (3,715). Intrusion (4,326) was the highest in 2012 and intrusion attempt (1,805) was highest in 2018, while malicious code (1,751) ranked highest in 2013. The trend overall shows that Fraud incidents across 2010-2018 consistently ranked the highest in incident reports with current 2018 statistics showing an increase in cyber harassment, intrusion attempt and malicious code incidents.

Table 1. Top five reported incidents MyCERT 2010-2018

	2010	2011	2012	2013	2014	2015	2016	2017	2018
Fraud	2212	5328	4001	4485	4477	3257	3921	3821	5123
Intrusion	2160	3699	4326	2770	1125	1714	2476	2011	1160
Intrusion Attempt	685	734	67	76	132	303	277	266	1805
Spam	1268	3751	526	950	3650	3539	545	344	356 (Cyber Harassment)
Malicious Code	1199	1012	645	1751	716	567	435	814	1700

Source: MyCERT Incident Statistics 2018

Table 2. MyCERT total reported incidents 2010-2018

	2010	2011	2012	2013	2014	2015	2016	2017	2018
Total	8090	15218	9986	10636	11918	9915	8334	7962	10699

Source: MyCERT Incident Statistics 2018

According to MyCERT in Table 2 above, in 2018, the total reported incidents amounted to 10,699. This increase since 2017 shows that although Malaysia is ranked third overall according to the GCI, the country is still vulnerable to cyberattacks and must stay vigilant in order to fight the ongoing battle against cyber criminals. Possibly because while both companies and educational institutions allow their employees and students to bring their own devices i.e. laptops, mobile phones to the workplace and educational environment, can ensure availability to knowledge it also may increase the chance of a cyber-attack on the institutional network (Ismail, Singh, Mustafa, Keikhosrokiani, & Zulkefli, 2017). The risk of having such policy in the workplace or educational institution, requires a policy or best practices for users of the network to prevent a cyberattack event to ensure a safer experience (Ismail et.al, 2017). That said, even with cyber laws in place, cybercrimes in Malaysia amounted to losses in 67.6 million Malaysian ringgit or USD 16.3 million as of April 2019. Previously, in 2018, cybercrime was responsible for almost 300 million Malaysian ringgit in losses or USD 72.3 million. The losses were due to mainly fraud cases i.e. telephone scams, e-commerce scams, e-financial fraud, credit card fraud etc. Despite reports of the Malaysian government's initiatives to bring awareness of cybercrimes to the public, Malaysian citizens continue to experience increasing cybercrimes as shown in Table 1 and Table 2 above. The next section includes the pertinent Malaysia Cyber laws and current cybercrimes in Malaysia.

MALAYSIA CYBER LAWS

The Malaysia cyber laws were established since the inception of MSC Malaysia. In the subsequent paragraphs, the main points of each cyber law, National policy and Penal Code most relevant to current cybercrimes in Malaysia will be highlighted and discussed (Computer Crimes Act 1997, Communications and Multimedia Act 1998, Copyright (Amendment) Act 1997, Personal Data Protection Act 2010, National Cyber security Policy and Penal Code).

Computer Crimes Act 1997

The Computer Crimes Act 1997 is a law “to provide for offences relating to the misuse of computers.” The Act was effective as of the June 1, 2000 and covers “unauthorised access to computer material, unauthorised access with intent to commit other offences and unauthorised modification of computer contents.”

The Computer Crimes Act 1997 was written to protect citizens from crimes concerning the misuse of computers. Computer Crimes Act section 9(1) states that “offences apply regardless of the nationality or citizenship, outside or within Malaysia.” This is a clear statement in the Act to protect Malaysians due to the borderless nature of the Internet. Thus, the Act applies to offenders outside Malaysia as well.

The offences are listed below along with their respective penalties upon conviction under the Malaysian Computer Crimes Act 1997:

1. **Section 3:** Unauthorized access to computer material
 - a. Section 3(3) fine not exceeding RM50,000 (approximately USD12,000) or imprisonment for a term not exceeding five years or both
2. **Section 4:** Unauthorized access with intent to commit or facilitate commission of further offence
 - b. Section 4(3) fine not exceeding RM150,000 (approximately USD36,000) or to imprisonment for a term not exceeding ten years or to both
3. **Section 5:** Unauthorized modification of the contents of any computer
 - c. Section 5(4) fine not exceeding RM100,000 (approximately USD24,000) or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding RM150,000 or to imprisonment for a term not exceeding ten years or both, if the act is done with the intention of causing injury as defined in the Penal Code
4. **Section 6:** Wrongful communication
 - d. Section 6(2) fine not exceeding RM25,000 (approximately USD6,000) or to imprisonment for a term not exceeding three years or to both
5. **Section 7:** Abetments and attempts punishable as offences
 - e. s.7(2) liable to the punishment provided for the offence: provided that any term of imprisonment imposed shall not exceed one-half of the maximum term provided for the offence

The cases below are examples of most recent computer crime cases in Malaysia.

In 2016, *Basheer Ahmad Maula Sahul Hameed v. Public Prosecutor*, the accused persons were convicted under section 4(1) of the Computer Crimes Act 1997 for wrongfully using a debit card belonging to an airplane accident victim to withdraw cash from an ATM machine and for transferring money from several other victims' online banking accounts without authorisation.

In 2016, *Rose Hanida Binti Long v. Pendakwa Raya*, the accused was charged under the Computer Crimes Act 1997 section 4 and Penal Code section 420 for using her superior's account and password without his knowledge. The High Court Judge sentenced her to 6 years imprisonment and fine of 260,000 Malaysian ringgit or 62,700 USD in default of 15 months jail due to the seriousness of the offence.

In 2016, *Public Prosecutor v. Roslan and Anor*, the accused who was an IT Systems Analyst for the Malaysian Hajj Pilgrims Fund Board, was convicted under Computer Crimes Act 1997 section 5(1) for modifying customer records in the organisation's database without authorisation.

In 2016, *Public Prosecutor v. Vishnu Devarajan*, the accused was charged under section 5 of the Computer Crimes Act 1997 for committing the following without authorisation: downloading and

launching software; running and stopping certain processes on servers; and running certain programs on the database server of a broadcast centre.

However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

In 2017, *Kangaie Agilan Jammany v. Public Prosecutor*, the accused, an Air Asia employee was charged under section 5 of the Computer Crimes Act 1997 for making modification of the contents of Air Asia's flight booking system without authorisation. The accused had allegedly used the function "move flight function" to make unauthorized modifications to passengers; flight schedules. The function allows authorised staff to make changes so that no charges are made to customers. In this case, the accused misused another staff's agent code to help his family members and friends to get discounted airline tickets. Due to this action by the accused, Air Asia alleged that the company lost about RM229,100 or USD 55,300. Both the Sessions Court and High Court found the accused guilty.

In 2018, *Public Prosecutor v. Datuk Gee Siew Yee*, the accused was charged with accessing a computer without authorization under section 3(1) of the Computer Crimes Act 1997. She was accused of unauthorised access to a computer that belonged to IT manager Brian Periera, with intent to access three files pertaining to Kelab Taman Perdana Diraja (Royal Lake Club) meetings.

As seen in the above cases, the charges were under sections 3,4, and 5 and as mentioned in the previous section, statistics on intrusion attempts have increased in 2018. Due to this, the fines and penalties may need to be reviewed. Awareness training for both private and public sectors and beginning at the academic level could also help as preventive measures.

Communications and Multimedia Act 1998

The Communications and Multimedia Act (CMA) 1998 is the law to "regulate the converging communications and multimedia industries, and for incidental matters."

The Act came into effect on April 1, 1999, and "provides a regulatory framework to cater for the convergence of the telecommunications, broadcasting and computing industries." The Act encompasses communications over the electronic media and regulates the activities by "network facilities and service providers, application/content application services providers" (Manap, 2015).

As stipulated, the Act was established in 1 November 1998 and since then, cases have been taken to the court under section 211 "Prohibition on provision of offensive content" and section 233 "Improper use of network facilities or network systems" of the CMA 1998. In January 2016 to July 2017, a total of 227 cases involving misuse of social media and websites were investigated according to Deputy Communications and Multimedia Minister Datuk Jailani Johari. "19 cases were compounded and eight prosecuted and convicted" Jailani said.

On February 20, 2018, Fahmi Reza was imprisoned for one month and fined 30,000 Malaysian ringgit or USD 7,238 for posting an edited version of then Prime Minister Najib Razak on social media. Fahmi was charged under Section 233(1)(a) of CMA 1998 and punishable under Section 233(3) for posting the image of the Prime Minister as a clown. Under the Act, Fahmi was guilty of transmitting content that is "obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person".

In *Nik Adib Bin Nik Mat v. Public Prosecutor*, the accused was charged under section 233(1)(a) of the CMA for sending indecent and false photos of cabinet leaders titled "Pesta Bogel" on Facebook. He was also charged under section. 5(1)(a) of the Film Censorship Act 2002 for possession of 883 pieces of pornographic videos in his laptop. The Session Court sentenced him to the maximum sentence of one year imprisonment for the first offence and another year imprisonment for the second offence. On appeal,

the High Court sentenced the accused to one week imprisonment and a fine of 3,000 Malaysian ringgit or approximately USD 724 in default 3 months imprisonment for the first charge and for the second charge, a fine of 10,000 Malaysian ringgit or approximately USD 2,400 in default 1.5 years imprisonment.

CMA has recently been discussed by the Malaysian government. In 2018, the Communications and Multimedia Minister, Gobind Singh Deo said that the new government Pakatan Harapan's (PH) manifesto called to repeal and amend the legislation to remove elements that are draconian. In the past, section 233 was primarily used to charge opposition members against the government. The minister mentioned that the government will look into section 233 to tighten the legislation to ensure fairness in regulating multimedia. This is a good way forward for Malaysia in revisiting the CMA and amending/repealing parts of the legislation to make it a more effective.

Copyright (Amendment) Act 1997

The Copyright (Amendment) Act 1997 is the law “relating to copyright and for other matters connected therewith.”

The Copyright (Amendment) Act 1997 amended the Copyright Act 1987 and came into force on April 1, 1999 to “make unauthorised transmission of copyright works over the Internet an infringement of copyright”. Copyright (Amendment) Act 1997 s. 7 states that the following are eligible for copyright: “literary works, musical works, artistic works, film, sound recording and broad casts”. However, s. 7(3) of the Act states that the above works are not eligible for copyright unless:

1. Sufficient effort has been expended to make the work original in character; and
2. The work has been written down, recorded or otherwise reduced to material form.

Therefore, according to the Act, an idea be it of the eligible works described above, may not be copyrighted unless s.7(3)a and s.7(3)b are satisfied.

The Act specifically states that a qualified person is the author if the work:

Section 10(1) states that copyright shall subsist in every work eligible for copyright of which the author or in the case of a work of joint authorship, any of the authors is, at the time when the work is made, a qualified person.

Eligible work for copyright also applies to work created in Malaysia as described in section 10(2) whereby:

1. Being a literary, musical or artistic work or film or sound recording is first published in Malaysia;
2. Being a work of architecture is erected in Malaysia or being any other artistic work is incorporated in a building located in Malaysia;
3. Being a broadcast is transmitted from Malaysia.

Section 41 of the Copyright (Amendment) Act 1997 describes the offences, which include:

Any person who:

1. Makes for sale or hire any infringing copy;
2. Sells, lets for hire or by way of trade, exposes or offers for sale or hire any infringing copy;

3. Distributes infringing copies;
4. Possesses, otherwise than for his private and domestic use, any infringing copy;
5. By way of trade, exhibits in public any infringing copy;
6. Imports into Malaysia, otherwise than for his private and domestic use, an infringing copy;
7. Makes or has in his possession any contrivance used or intended to be used for the purposes of making infringing copies;
8. Circumvents or causes the circumvention of any effective technological measures referred to in subsection (3) of section 36;
9. Removes or alters any electronic rights management information without authority; or,
10. Distributes, imports for distribution for communicate to the public, without authority, works or copies of works in respect of which electronic rights management Information has been removed or altered without authority.

If any person is found guilty of any of the offences (a-j) described above, then he will be subject to according to the Act:

A fine not exceeding: ten thousand ringgit for each infringing copy, or to imprisonment or a term not exceeding five years or to both and for any subsequent offence, to a fine not exceeding twenty thousand ringgit for each infringing copy or to imprisonment for a term not exceeding ten years or to both.

However, for an offence under paragraph g:

A fine not exceeding twenty thousand ringgit for each contrivance in respect of which the offence was committed, or to imprisonment for a term not exceeding ten years or to both and for any subsequent offence to a fine not exceeding forty thousand ringgit for each contrivance in respect of which the offence was committed or to imprisonment for a term not exceeding twenty years or to both.

The following are examples of cases under the Copyright (Amendment) Act 1997:

In 2009, *Chuah Gim Seng & More Again v. SO*, the accused were found guilty and convicted for the sale of pirated copy films. The penalty imposed was RM2,000 (approximately USD480) for the sale of each copy and in default a four-month jail term for failure to pay each charge.

In 2011, *Public Prosecutor v. Haw Swee Po*, the accused was tried for possession and use (other than for private and domestic use) of 3,300 copies of seven films in DVD format. The court sentenced the accused to 14 months' imprisonment.

Copyright infringement cases as mentioned above still remain and are practiced frequently. The fines and penalties for this crime should be reviewed and increased. Moreover, awareness training on wrongful use of pirated films should be made more public and discouraged to prevent future copyright infringement cases.

Personal Data Protection Act 2010

The Personal Data Protection Act 2010 is the law to “regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.” The Act does not include the Federal and State governments according to section 3(1).

The Act is based on seven principles:

- General Principle
- Notice and Choice Principle
- Disclosure Principle
- Security Principle
- Retention Principle
- Data Integrity Principle
- Access Principle

According to Section 2(1), this Act applies to:

1. Any person who processes; and
2. Any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions.

Section 2(2) describes the application and jurisdiction purposes whereby:

1. The person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or
2. *The person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.*

Section 3(2) of the Act states that “any personal data processed outside Malaysia shall not apply unless that personal data is intended to be further processed in Malaysia.”

Furthermore, s. 6(3) of the Act states that personal data shall not be processed unless—

1. The personal data is processed for a lawful purpose directly related to an activity of the data user;
2. The processing of the personal data is necessary for or directly related to that purpose; and
3. *The personal data is adequate but not excessive in relation to that purpose.*

The first case to be charged under the Personal Data Protection Act 2010 occurred on 3 May 2017. Khas Cergas Sdn Bhd, which operates Victoria International College, was charged in the Sessions Court for processing personal data of former employees of the college without a valid certificate of registration issued by the Personal Data Protection Department (PDPA), in violation of section 16(1) of the PDPA. Section 16(1) requires certain classes of data users to be registered and to be issued with a valid certificate of registration by the PDPA.

This legislation is relevant only to institutions, organizations handling personal data in commercial transactions. Although training on PDPA and public awareness is made of the law in Malaysia, the case of Victoria International College still occurred. The law may need to be reviewed if not for its current fines and penalties, but for its definition of personal data. In this digital age, use of personal data in the internet for identification purposes is common place and PDPA has yet to include “biometrics” or a definition referring to such traits in the legislation.

Malaysian Penal Code

The Malaysian Penal code is the law relating to criminal offences. It is with this law that criminal offences not covered in the previous cyber laws discussed can convict offenders for crimes such as sale / distribution of pornography, ransomware, and fraud. The below sections from Penal Code describes the applicable sections:

Section 292 is the selling, distribution, or public exhibition of obscene materials.

For this offence if convicted, the offender shall be imprisoned for a term “which may extend to three years or with fine or with both.”

Section 293 is the selling, distribution of obscene materials to minors or a “person under the age of twenty” years old or offers or attempts to do so.

For this offence if convicted, the offender shall be imprisoned for a term, which may “extend to five years or with a fine or with both”

Section 383 states that “whoever intentionally puts any person in fear of any injury to that person or to any other, and thereby dishonestly induces the person so put in fear to deliver to any person any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits ‘extortion’.”

The punishment for extortion as stated in s. 384 “imprisonment for a term which may extend to ten years or with a fine or with whipping or with any two of such punishments.”

Section 416 states that “any person is said to ‘cheat by personation’, if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.” The offence of cheating by personation is punishable with imprisonment for a term which may extend to seven years and/or a fine.

Section 422 states that “whoever dishonestly or fraudulently prevents any debt or demand due to himself from being made available for his creditors shall be punished with imprisonment for a term which may extend to five years or with a fine or with both.”

Section 424 states that “whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment for a term which may extend to five years or with fine or with both.”

In 2016, *Public Prosecutor v. Charles Sugumar a/l M. Karunnanithi*, the accused tour driver was charged under section 424 of the Penal Code for dishonestly concealing money of a scam victim in his bank account. The victim had befriended a person by the name of Alfred Hammon from UK through Facebook. Alfred Hammon then made the victim transfer money to the accused’s bank account based on the pretence that he needed the money to cash a USD 3 million cheque and would return the money with interest. The Magistrate acquitted the accused and found that the accused was made a scapegoat by the customer who took advantage of his kindness.

The Malaysian Penal Code is the catch all legislation whereby for cases not covered by current Malaysian Cyber Laws, can be charged under. Although this may be a convenient at the moment, a more practical cyber law should remain in place to cover such charges. This law should also be periodically reviewed to keep up with current cybercrimes and relevant offences.

The cases and laws previously stated are not without national law enforcement agencies working with their international counterparts. In Malaysia, these agencies are the Royal Malaysian Police, National Cyber Security Agency, Cyber Security Malaysia, and Cyber999. Most recently, the National Cyber Security Agency of Malaysia was established as the leading agency to handle cyber security matters. The next section describes the agency and its functions.

National Cyber Security Agency

In February 2017, the National Cyber Security Agency (NACSA) for Malaysia's leading agency was established to handle cyber security matters, with the objectives of "securing and strengthening Malaysia's resilience in facing the threats of cyberattacks, by coordinating and consolidating the nation's best experts and resources in the field of cyber security" (National Cyber Security Agency, 2018)

National Cyber Security Policy

Vision Statement

Establishing a stable, safe and resilient cyber environment to meet the economic and social needs of Malaysia.

The Objectives of NACSA are:

- Address the risks to the Critical National Information Infrastructure (CNII)
- To ensure that critical infrastructure are protected to a level that commensurate with the risks
- To develop and establish a comprehensive program and a series of frameworks

The National Cyber Security Policy (NCSP) was developed based on a framework that comprises legislation and "regulatory, technology, public-private cooperation, institutional, and international aspects" (National Cyber Security Agency, 2018, December 6).

The ten sectors of the Critical National Information Infrastructure (CNII) that NCSP seeks to address the risks to are:

- National Defence and Security
- Banking and Finance
- Information and Communications
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency Services
- Food and Agriculture

NACSA's mission is to be committed towards the implementation of the national cyber security policy and management in an integrated and coordinated manner.

The NACSA's national cyber security policy comprises of Eight Policy Thrusts, which are:

Effective Governance

National cyber security initiatives are centralised with effective cooperation between public and private sectors and establish formal and foster informal information sharing

Legislative and Regulatory Framework

Enhance/review cyber laws to focus on the dynamic nature of cyber security threats and ensure legislations adhere to international treaties and conventions

Cyber Security Technology Framework

Ensure legislation is adheres to international laws, treaties and conventions and application of an evaluation/certification program for cyber security products and systems

Culture of security and Capacity Building

Develop and foster a national culture of security whereby cyber security awareness and education programs across CNII are standardised and such knowledge dissemination is effective at the national level

Research & Development Towards Self-Reliance

Strengthen the cyber security research community by “promoting the development and commercialization of intellectual properties, technologies and innovations through focused research and development” and foster the advancement of cyber security industry

Compliance and Enforcement

Develop standardised cyber security systems to strengthen the monitoring and enforcement of standards and create a standard of cyber security risk assessment framework

Cyber Security Emergency Readiness

- Strengthen the national computer emergency response teams (CERTs)
- Develop effective cyber security incident reporting mechanisms
- Encourage all elements of CNII to monitor cyber security events
- Develop a standard business continuity management framework
- Disseminate vulnerability advisories and threat warnings in a timely manner
- Encourage all elements of the CNII to perform periodic vulnerability assessment program

International Cooperation

- Encourage active participation in all relevant international cyber security bodies, panels and multi-national agencies
- Promote active participation in all relevant international cyber security by hosting an annual international cyber security conference

NACSA is still at its infancy and the country has yet to experience its effectiveness in handling cybersecurity matters and the effectiveness of its national strategy. The National Cyber Security Strategy will be issued by NACSA in mid-2019 according to Deputy Prime Minister Dr. Wan Azizah Wan Ismail. Of note, one of the main activities outlined in the National Security Council Directive is to implement a National Cyber Crisis Training Charter to test the effectiveness of procedures and familiarize CNII agencies with cyber incident handling.

SOLUTIONS AND RECOMMENDATIONS

The cyber security legislations of Malaysia require an on-going review as cybercrimes continue to grow and evolve as evidenced in the statistics and cases stated above. The Internet has both its positive and negative aspects. While it can be used for convenience and ease of use such as internet banking and e-commerce, the data a user provides to enter the website can be easily plucked by cyber criminals. In order for users to feel safer, they must practice safe cyber security housekeeping. This can be done by conducting knowledge sharing at the most basic level in schools to employee training during their first days of orientation in a new company. However, to ensure this practice is implemented, a national policy should include this standard training for every company and institution using computers. The National Cyber Security Policy has good aspects to its framework, however the policy is to be implemented only in mid-2019. The NACSA has only been established since 2017 and it is too early to say the effectiveness of the organisation. Imposing higher penalties on those convicted of cybercrimes may need to be implemented in the current legislation or future legislations to prevent criminals from doing the crime. Privacy under the PDPA 2010 is only applicable to companies handling personal data for commercial transactions and a definition under the Act is absent for biometric data. This aspect of PDPA should be reviewed in order to include all forms of personal data is protected under the PDPA.

FUTURE RESEARCH DIRECTIONS

Currently there is limited research in the area of cybersecurity in Malaysia. Future research in both qualitative and quantitative should be looked into and focus on law enforcement and effectiveness of current legislations.

CONCLUSION

Malaysia has great initiatives when it comes to their cyber security laws. The dedication of the country to provide a secure network environment is promising, with Malaysia establishing NACSA to lead in all cyber security aspects for the nation. Their national strategy is also said to be issued in mid-2019, which will further enable the government agency clear guidance on how to handle cyber security matters. However, with the advancement of technologies and the enthusiasm of the public to use technology, criminals will always find a way to leverage this for themselves. That is the reason why Malaysia must continue to stay vigilant and continue to review their legislations to protect their citizens from cyber criminals.

REFERENCES

Communications and Multimedia Act 1998.

Computer Crimes Act 1997.

International Telecommunication Union (ITU). (2017, July 6). *Global Cybersecurity Index 2017*. Retrieved from <https://www.itu.int/en/ITU-D/Pages/publications.aspx#/publication/59dae8cf13659441249d2fa9>

Ismail, K. A., Singh, M. M., Mustafa, N., Keikhosrokiani, P., & Zulkefli, Z. (2017). Security Strategies for Hindering Watering Hole Cyber Crime Attack. *Procedia Computer Science*, 124, 656–663. doi:10.1016/j.procs.2017.12.202

Malaysia Penal Code Manap, N. (2015). Alignment of Malaysia and Asean Agreements on Ict Laws: A Review. *Brawijaya Law Journal*, 2(1). <https://doi.org.proxyvlib.mmu.edu.my/10.21776/ub.blj.2015.002.01.01>

MyCERT Incident Statistics. (2018). Retrieved December 6, 2018 from <https://www.mycert.org.my/statistics/2018.php>

National Cyber Security Agency (NACSA) Malaysia. (2018, December 6). Retrieved from <https://www.nacsa.gov.my>

Personal Data Protection Act 2010.

ADDITIONAL READING

Beatty, D. L. (1998). Malaysia's Computer Crimes Act 1997 Gets Tough on Cybercrime but Fails to Advance the Development of Cyberlaws. *Pacific Rim Law & Policy Journal*, (2), 351.

Grabosky, P. N., & Broadhurst, R. G. (2005). *Cyber-crime : The Challenge in Asia*. Hong Kong: Hong Kong University Press.

Tan, S. L. O., Khan, S., & Reza, M. H. (2012). *Cybercrime and Cyber terrorism : the security measure in Malaysia*. Lambert Academic Publishing, c.

Zain, A. M., Jaafar, F., Fauz, F. H. A., Ramli, W. N. R. W., Lugiman, F. A., & Saberi, N. E. (n.d.). Social media and cyber crime in Malaysia. *Springer Singapore*. doi:10.1007/978-981-287-332-3_53

KEY TERMS AND DEFINITIONS

Cyber Security: The practice of defending computers and related systems mobile and fixed from attacks against hackers and cyber criminals.

Cyberattack: The act of hackers to disrupt or damage a computer network or system.

Cybercrimes: Criminal activities using the internet as a vehicle to commit the crime.

Fraud: The act of deceiving for personal monetary gain.

Intrusion: Wrongfully accessing a computer's system or network.

Malicious Code: Computer code often used by hackers to infiltrate a computer to cause damage and security vulnerabilities.

Spam: Messages sent via the internet often unimportant with the intent to advertise, induce malware and phishing programs.

Game Console Protection and Breaking It

2

Nezer Jacob Zaidenberg

College of Management, Israel

INTRODUCTION

This chapter presents a survey of the attacks and defenses on various video game consoles (hereby consoles). Consoles are complex embedded systems designed to run various video games. At the console release time, the console is comparable to a high-end gaming PC. In addition to gaming hardware, the console also features an operating system and libraries. Unlike general-purpose PCs that run just about any software, consoles are supposed to run only licensed code and games. Consoles also include complex Digital Rights Management (DRM) and copy protection mechanisms. The attacks presented here are usually geared toward running custom OSs, homebrew (unlicensed) software and pirated games on the console. Over the last 20 years, various groups discovered the attacks against different consoles. Most of the attacks were reported by in the annual CCC conference.

The survey focuses on recent generations of game consoles (6th, 7th and 8th generation) as these are more interesting from a console hacking perspective. Prior console attacks usually used custom hardware modifications (modchips). These attacks are not comparable to attacks on newer generations, and therefore, older consoles are beyond the scope of this chapter. Also, this chapter does not deal with mobile consoles. (Such as PSP, Vita, Nintendo DS etc.) Last, Many other devices that can be considered gaming devices, particularly mobile phones (iPhone/Android). Also, PC-gaming is very common. (and PC games also suffer from piracy). These devices are not considered game consoles and are beyond the scope of this chapter.

BACKGROUND

Consoles are a type of embedded system. Consoles offer processing capacities similar to a high-end PC.

However, unlike PCs, consoles hardware is geared entirely to run video games. At the time of release, consoles offer CPU, RAM, graphics capabilities and hard drive capacity comparable to a gaming PC. Furthermore, most consoles are cheaper than a comparable PC as the consoles' manufacturers subsidize consoles. The manufacturers sell the game consoles at a loss. Instead of profiting on console sales, the consoles' manufacturers profit when the users buy games.

Tools to attack the copy protection on consoles are as old as consoles themselves. However, the rising popularity of recent consoles has transferred the manufacturing modchips and tools to break the game console copyright protection is a flourishing business. As piracy is illegal, there are no official figures. However, the market size is significant. Console modchips cost roughly 50 USD apiece. Console sales often reach quantities of 40M to 100M units per model or even more in some cases. Most of these consoles are fitted with modchip at some point. These figures suggest that the modchip industry is a multibillion USD industry.

DOI: 10.4018/978-1-5225-9715-5.ch031

Legality

It is of course illegal to pirate games. However, it is legal for the end-user to modify equipment that he (the end-user) owns. (fair use) Such modification can be, for example, installing modchips or software, provided the goal is not running pirated software but running homebrew code or Linux. It is also legal for the end-user to create backups of CDs that the end-user owns. (Playing backup CD is identical from a technology standpoint to playing a copied CD)

Installing modchips creates a loophole because, in the United States and other jurisdictions, thanks to the Digital Millennium Copyright Act (DMCA) it is also illegal to create devices whose sole purpose is to break DRM (such as modchips) even if no piracy is committed. So, in the United States, selling modchips designed to copy games is also illegal. Other countries have different laws and, in some jurisdictions, selling modchips may be legal. This chapter focuses on the technology of attacks and defenses. The complicated international legal aspects of DMCA and game consoles are beyond the scope of this chapter.

Usually, modern console attacks no longer require modchips. However, it is worth noting that in 2011, Sony sued George Hotz (geohot) over DMCA violations regarding published PS3 attacks without using any modchip or hardware modifications.

The case was settled outside court, and Hotz committed not to hack another Sony product.

However, even software-only attacks (i.e. running code that the user has coded on an embedded device that the user owns) may result in legal action, in the USA.

Motivation

The obvious motivation beyond attacks on game consoles is piracy. Console games are expensive. Console games are even more expensive than PC games. The PC version of the same game is usually cheaper than the console version due to royalties collected by the console manufacturer to cover the subsidized cost of the console itself.

However, in addition to piracy, there are several other motivations behind attacking game consoles. The first of those is running other operating systems, usually Linux. As game consoles offer high-end (for the release time) hardware at subsidized costs using game consoles as regular computers and running Linux has appealed to hackers. Furthermore, according to DMCA, it is considered legal and fair use of the end-user equipment. The console manufacturer attempts to prevent running Linux as console games will not be purchased for Linux servers. Since the console itself is subsidized the manufacturer loses money if the end-user installs Linux on the console.

Another potential motivation is running homebrew software, i.e. software that the user coded (or open-source software the user compiled) on its own machine. This use case is also legal, according to DMCA. I.e. it is considered fair use.

There are two risks from the console manufacturer point of view with running homebrew code.

The first is unlicensed games. The console manufacturer is subsidizing the console sales but collecting royalties from any game sold. This is possible only because the manufacturer has complete control (using signatures) on what is allowed to run (whitelisted, signed) to run on the machine. Unlicensed games don't allow the manufacturer to collect royalties. Therefore, unlicensed games without paying royalties should not be allowed to execute on the machine.

The second problem with homebrew code is that it removes the manufacturer control over the entertainment system at the end-user's digital home. Console manufacturers frequently have additional goals in this field (enforcing standards, formats, operating systems to use etc.) Therefore, the console users

must use signed software controlled by the manufacturer. By allowing homebrew software, the console vendor loses control on the end-user digital home.

5th GENERATION AND OLDER CONSOLES

5th generation and older consoles did not have hard drives. Games were only distributed on proprietary cartridges or CDs. Older consoles (like Sony PlayStation etc.) were hacked almost entirely for software piracy purposes. These hacks were usually committed using modchips.

Modchips

Most consoles used off the shelf CPUs and other components. Using off the shelf components was inexpensive compared to custom components. However, off the shelf components did not provide proper copy protection mechanisms.

To provide copy protection, the older console had software running on top of an EPROM or BIOS chip that enforced copy protection. These chips were used only for copy protection and some simple functions (such as booting) and were not required for standard operations. “Modchips” were tiny electronic boards that were soldered to the game console board and circumvented the copy protection chip. The modchip often replaced another chip. The modchip then performed as the chip that it was supposed to replace. However, the modchip would not enforce copy protection. Opening the console box, cutting wires and replacing chips would void the console warranty. (but apparently, in many cases the end-user would not care).

Modern consoles are usually protected using software means (as opposed to hardware chip), and thus modchips are no longer used on modern consoles.

6th GENERATION CONSOLES

Xbox

Michael Steil offered a detailed summary of the Xbox weaknesses and design problems (Steil 2005). Microsoft wanted to release a console competing with Sony’s PlayStation 2 under a tight schedule. The tight schedule requirement led to a game console design that is closely related to a windows PC. (As Microsoft already had the source and capabilities for PC operating systems for games.)

The Xbox is running on top of almost a standard PC hardware for the time.

The Xbox includes an Intel Celeron III CPU, NVidia GeForce GPU, hard drive and memory (64MB of RAM).

This led hackers to the conclusion that “the Xbox is a PC”.

PCs, and thus the Xbox, have multiple legacy components. These components were later used to hack the Xbox and alter its behavior. The Xbox design had several critical mistakes (Steil’s paper provides a complete list) including

- Multiple design mistakes
- Failure to analyze attacker resources and attack vectors properly

- Implementation errors
- Failure to do sufficient audit possible due to release schedule requirements
- Failure to handle security incidents properly.

As a result of these errors, the Xbox hackers managed to hack the Xbox quite quickly.

Currently, the Xbox security is completely broken. Users can run pirated copies, homebrew software and Linux without even opening the Xbox.

Game Cube

The GameCube was released in 2001 by Nintendo. The game cube is a PowerPC G3 (PowerPC 756e codename Geko) running at 485 mhz with 40MB. The GameCube was comparable to PowerPC based macs released by Apple circa 2001. The GameCube provided attractive hardware for running homebrew applications much cheaper than comparable macs. The GameCube CPU is comparable to the Apple G3 CPU and includes MMU, vector processor features etc.

The GameCube included a DVD copy protection system in the DVD firmware. The DVD firmware refuses to boot from standard DVD. However, GameCube's DVD protection is faulty. The GameCube DVD had two major backdoors that could be used for attacks allowing modchips.

The DVDs of the GameCube were signed on manufacturing using some measurement of the recorded disc. This measurement could not be measured and replicated accurately. If a game is copied, then these measurements would be slightly different on the copy compared to the original these differences result in different signatures.

Thus, original games could be separated from copies. (SecureROM used similar protection for PC games)

For such protection to work the signature should have been using an asymmetric cypher, so the verification and signing key would be different. Different keys mean that the signing and verification keys are different.

If the signing and verification keys are identical, the manufacturer can sign the masters using a private key that is not revealed to the users. When using the same key for signing and verification (symmetric encryption), the user can calculate the new signature and sign self-created copies. Nintendo used symmetric cypher with the key stored that is stored on the DVD itself. Therefore, this protection was useless as the user could calculate and replace the signature.

Additionally, the GameCube DVD had a backdoor password attack that allowed modchips. The password was broadcasted to the DVD to state the disc is verified. The password was compared on the DVD using memcmp(3) function. Hackers revealed the password using a timing attack. Thus, the GameCube password was revealed.

Today the GameCube security is completely broken. Since users can sign their own copies, Users can run pirated copies, homebrew software and Linux without even opening the GameCube.

For further reading on GameCube protection, please refer to Domke et al. 2004.

Playstation 2

The PlayStation 2 (hereby PS2) is the bestselling game console of all times. There were over 150 million PS2 consoles sold worldwide.

The PS2 came with 299MHz MIPS based core (emotion engine), 32 MB of RAMBUS RAM and GPU clocked at 147 Mhz. The PS2 came without a hard drive by default but allowed for an optional hard drive.

Sony released Linux for PS2 on their own.

Most PS2 attacks were based on modchips that allowed pirated games to run. Sony has created several revisions to the console board and bios each time eliminating some of the modchips. The hacker community reacted with introducing new modchips to the revised board edition.

Brown 2003 offers a summary of the PS2 modchip efforts.

Today most PS2 that are still working are fitted with a modchip.

SEGA Dreamcast

Sega Dreamcast was the last console that Sega ever designed. It was released in 1998 and discontinued in March 2001 (before other “6th generation” consoles were even released). The Dreamcast had 200Mhz, 16MB of RAM. Like many old-consoles (such as the original PlayStation, Nintendo 64 etc.) the Sega Dreamcast was vulnerable to modchips attacks that allowed users to play pirated copies.

7TH GENERATION CONSOLES

Nintendo Wii

The Nintendo Wii was the first and most successful of the 7th generation consoles. It was released about a year ahead of its peers. (The PS3 and the 360) The Wii was very cheap compared to its competitors (The. 360 and PS3) and offered a unique playing experience using an innovative controller.

The Nintendo Wii is running on hardware similar to its predecessor, the GameCube.

The Wii's CPU is PowerPC G3 (same as the GameCube), but the Wii's CPU is clocked faster.

The Wii also has a similar memory structure in several memory banks. The Wii's extended memory bank offers 64 MB of memory in addition to 24MB main memory for a total 88 MB of memory. Thus, the Wii has 48MB more than the GameCube that had only 16MB of extended memory for a total of 40MB.

Unlike other consoles, the Wii was not sold at a significant loss, and thus hackers had less of motivation to purchase the Wii and use it as a Linux box.

The Wii software allows the execution of GameCube games in a “compatibility mode” that is identical to GameCube by simply downscaling the CPU and thus attacks that target the GameCube were also tested on the Wii. Most GameCube attacks worked on the Wii. Thus, Nintendo's Wii was partially broken on release as it was running the GameCube code and pirated GameCube copies (using faulty symmetric password mechanism) on compatibility mode.

Thus the Wii could run GameCube code and pirated copies but not homebrew code.

Hackers introduced the Twizzers attack to bypass the GameCube mode limitations.

Nintendo off course knew about the GameCube vulnerability at the time of the Wii release. However, since the GameCube was limited to only 16MB of RAM, Nintendo assumed that the rest of the memory is safe. Thus, Nintendo used the other 48MB for security purposes.

However, The PowerPC CPU on the Wii (like any other CPU) had an address line. In order to bypass the 16MB limitation of GameCube hackers used tweezers on the wii motherboards hackers to shorten the address lines. Thus hackers managed to move the 16MB that GameCube mode can access to other addresses physical address. Thus, hackers were eventually able to map and dump the entire Wii memory.

The memory that they dumped contained all the encryption keys.

The Wii keys that were now dumped allowed access to the ECC (elliptic curve cryptography) (Miller 1985) private key of the specific machine as well as the public key of Nintendo. It also contains AES and HMAC keys, The common key (for all Wii), the SD key and the root key. These keys were hardcoded in the Wii Operating System (IOS) and on a write once ROM.

Today, The Wii is still cracked for piracy and running homebrew and Linux.

The CCC console hacking lecture from 2006 describes breaking the Wii protection in GC mode.

The CCC console hacking lecture from 2008 by Marcan et al describes the Twiizers attack.

According to Bushing et al 2010 there were over 1M users in the Wii homebrew channel.

Xbox 360

Learning from Xbox mistakes, The Xbox 360 is very different from a PC. The Xbox 360 runs on a 3-core IBM PowerPC processor (3.2 Ghz) 512 MB of RAM. SATA hard drive (size varies according to exact model) and R600-class GPU

The Xbox 360 includes several security features such as

1. Security Hypervisor a “Type-1” hypervisor
2. Encrypted memory (So sniffing the buses as was done in the original Xbox will not be fruitful)
3. Data execution prevention i.e. W^X on memory pages
4. E-Fuses – E-Fuses are specific memory that exist on the CPU itself that can be “burned” after burning a fuse it cannot be “unburnt” it remains, physically burned on the CPU. The only way to “unburn” the E-Fuse is to replace the CPU.
5. CPU ID – The Xbox 360 processor had sufficient CPU fuses that could create a unique cpu id for each cpd by burning different fuses for each Xbox 360

The main attack against the Xbox 360 was “The King Kong” attack. This attack uses the fact that the 360 does not encrypts all the memory. Some memory must remain unencrypted for DMA etc.

A game can copy to memory using the pixel shader, part of the Video adapter. (not all games but the “King Kong” game, for example, does not check the pixel shader) thanks to a bug in the hypervisor the user can create a hyper call that calls jump to the copied memory and run unencrypted code. Thus homebrew code and Linux can be started.

Microsoft released a patch for XBOX which also blocks Linux. Furthermore, the patch burns some E-Fuse on the CPU. If the user ever upgrades the software, downgrade is impossible because of the software will check the E-Fuse and will not boot. Another attack that was discovered allowed modchips for the DVD drives that allow for pirated copies.

The XBOX 360 is an exception in the console scene.

It was broken for game piracy relatively early in its life cycle but has not been broken for running Linux and homebrew code in any consistent way since. (Except for the King Kong attack (Anonymous 2006) described above that was blocked relatively early.)

The XBOX 360 remains an exception in that it still does not run homebrew code and Linux.

This section is based mainly on Felix Dumke’s summary (Domke 2006) with some addition from Dumke’s previous lecture. (Steil 2005)

Playstation 3

2

The PlayStation 3 (hereby PS3) is unique as it remained secure platform for over 4 years. Well over any other platform. For a time breaking the PS3 was the “Holy Grail” hackers aspired to break. More than 87 Million PS3 were shipped.

The PS3 is running on a cell processor which is a Power PC processor.

The CPU is augmented by 8 vector processors. These vector processors are called SPEs.

These SPE are a single prevision float point unit for video processing, for games.

However, out of the 8 SPU only 6 are available for games.

One SPU is automatically disabled by design on all PS3s. This allows Sony to use defective CPUs (with one SPE damaged) reducing the CPU manufacturing costs. An additional SPU is always used for encryption and decryption of instructions leaving 6 SPU for general purpose usage. The SPU also have curtained memory that allows some memory to be shadowed from other processes.

The PS3 offered also 512MB of memory, a hard drive (of various sizes) and was heavily subsidized by Sony.

The Sony PS3 included “Cell OS level 1” a type-1 hypervisor and “Cell OS level 2” OS.

Initially Sony allowed for “other OS” a limited (but sufficient) Linux support. However, hackers used subverting attacks, i.e attacks by the guest OS on the host hypervisor, to dump the code of the hypervisor. Following the subverting attacks, Sony decided to drop support for “other OS” feature.

The PS3 security system also includes signing executables, signing storage, a security SPU.

The first attack on PS3 was attacking the secure storage. The secure storage encrypts everything with the same key. By copying stuff to the hard drive (like a movie) the hacker gets the encrypted version of everything that was copied. By moving stuff on the HD and reading it (for example, as a movie) we can get the decrypted version of everything on the HD. So any encrypted file can be deciphered by moving it and reading it using another application. Thus the PS3 secure storage was broken.

The hypervisor mapping bug which lead to exposure of the hypervisor code work was discovered by George “geohot” Hotz. The method is similar method to the Wii “Twiiizer” attack. It is relying on the fact that we have second level address translation, i.e. double page tables. one page table exist in hypervisor mode and another page table exists in Supervisor (OS) mode. geohot was able to bypass the memory protection by getting a pointer to cell-OS level-2 memory location while Cell-OS level-1 (the hyper visor) thinks that the same memory location is free. Since the hypervisor thinks that the memory is free at some point the hypervisor will map the hypervisor stuff to this free address. But as the cell-OS level-2 is still mapping this memory address it can read from this address and that led to the hypervisor code exposure. But even though the hackers now had access to the hypervisor code that has not led to any significant attacks for quite a while.

The first meaningful attack against was the PS3 jailbreak.

The PS3 jailbreak is a USB dongle that acts as a USB hub simulating multiple USB devices behind the hub. The dongle is exploiting a bug in the Cell OS in handling USB devices. The PS3 Jailbreak dongle allowed execution of random code on the PS3. At this point piracy was possible.

Through a series of other discoveries hackers have found serious implementation flaw in the way SONY signed binaries. SONY implemented the Elliptic Curve DSA (ECDSA) algorithm to sign their ELF's. ECDSA is a strong crypto infrastructure and a method that is still considered unbreakable. However, ECDSA relies on random numbers. (Or pseudo random numbers) Sony's faulty random number generator is always initialized with the same string and returns identical pseudo random numbers. Thus,

Sony ECDSA implementation is faulty. The faulty elliptic curve implementation in Sony PS3 was broken and the keys were leaked.

The private keys of Sony PS3 was leaked to the internet by Geohot on 2011. (Hotz 2011) These keys cannot be banned or blacklisted by Sony because all the old consoles still use these keys and must still work.

Today, after the private keys leaked to the internet, it is possible to run any software for the PS3. Running homebrew or pirated code and even Linux on the PS3 is possible. It does not require opening the PS3 or installing any USB dongles or modchips.

The PS3 has complete analysis of its security system available on (Bushing et al 2010) this section is based on this presentation.

8TH GENERATION CONSOLES

8th generation game consoles are the most recent generation. The common factor in many attacks against 8th generation consoles is attacking the web browser (webkit) using well known browser or webkit weaknesses.

Wii-U

The Wii-U was released in November 2012. The Wii-U offered a Tri-core PowerPC chipset, 2GB of RAM. The Wii-U has already been cracked (to play pirated games) about one month after its launch (Sven et al 2013).

Unlike the Wii the Wii-U has not been commercially successful (Takahashi 2013). Only 3.61M units were sold until the end of June 2013 which is relatively low compared to Wii or other 8th generation consoles. still the Wii-U offered better hardware then the Wii and an exotic hacking opportunity.

The Wii-U include hardware and software similar to the Wii (only faster).

The Wii-U security system had been a victim to its predecessor weakness of backward compatibility. Just like the Wii was hacked first in GameCube mode the Wii-U was hacked using the Wii compatibility mode.

The hacking of the Wii-U was possible due to the fact the Wii-U also includes Wii OS that run on real mode. Even though the Wii-U will only boot an encrypted and signed code all Wii weaknesses still existed in Wii-U. Therefore, the hackers could learn the new security measures using the old Wii methods.

The hackers were able to create a timing attack against the Wii by replacing the instructions in memory after their signature were verified and decoded. Using some custom hardware hackers were able to dump the Wii-U boot ROM. Shortly afterwards the hackers attacked the PPC HRESET bus and received the keys for Wii mode. (At this point the hackers had complete administrator access on the hardware, but were limited in Wii mode)

The secondary weakness of Wii-U was the webkit web browser. The Wii-U is using webkit that is an open-source software project with known bugs, vulnerabilities and attacks databases. Using Wii and webkit issues the hackers obtained the means for entering and leaving virtual Wii mode.

Nintendo discontinued the unsuccessful console on 2017 after releasing the switch and selling only 13M consoles in almost 5 years. Today most of the protection of the Wii-U is completely hacked (and can run homebrew code and Linux). Furthermore, Wii-U games can be pirated.

PS4

The PS4 was released in 2013. The PS4 featured dual CPU each with 4 cores (1.6Ghz) and 8 GB of RAM. The hardware was refreshed (and marketed as PS4 Pro) with faster CPU and GPU on 2016. The PS4 design was based on past mistakes and most legacy components were removed. However, the PS4 used the webkit as a browser and FreeBSD as an operating system. Both FreeBSD and webkit are open-source software and both have known weaknesses. These weaknesses were used to hack the PS4 for piracy.

In order to boot Linux and run Homebrew code hackers had to reverse engineer massive part of the hardware and code platform specific parts into the Linux kernel. (Marcan 2016) Lecture details these efforts. Today PS4 can be hacked to run any software included pirated games and other operating systems (Linux). However, unlicensed platforms and operating systems are not allowed on Sony's play station network.

Xbox One

The Xbox One was released in 2013 and competed with the PS4 and Wii-U.

Upon launch, the system had an AMD CPU (1.75Ghz, 8 cores), AMD (ATI) graphics adapter, 8GB of RAM and various hard drive options. The system was re-launched as Xbox One S (August 2016) and Xbox One X (November 2017) featuring faster CPU and GPU, more RAM memory and faster Buses.

The Xbox One S is the most powerful console ever released at the time of writing this chapter. It is estimated that roughly 40M Xbox one units were sold.

The Xbox security is still unbroken (at the time of writing this chapter)

One of the main controversies involved with Xbox One and DRM is the game locking controversy.

A common practice among players is to play a game until one “finishes” the storyline of the game or is tired of it. After finishing the game, the player exchange the game in a local game store for another game or lend it to a friend. Thus, the game now has a new “owner” and a new user can play the game (though only one user can play the game simultaneously). Microsoft toyed with the idea of locking games to specific Xbox Live account eliminating the habit of lending or exchanging games. There was a tremendous public cry when the gamers found out about it (Matricker 2013) and Microsoft eventually backed down (Stuart 2013).

Nintendo Switch

Nintendo Switch (Hereby Switch) is a home/portable console that uses mobile hardware (ARM chips, battery etc.). The switch was unveiled on 2016 and released on 2017. It replaces the unsuccessful Wii-U. The switch offers 8 ARM cores (1 Ghz) Nvidia GPU and 4GB of RAM. It can be used both as a portable or stationary home console.

The Switch sold 23M units in about a year and a half since it was released much more than the Wii-U, that sold 13M units in 5 years.

In December 2017 9 months after the Switch release it was partially hacked by Plutoo et al. (Plutoo 2017) The switch suffers from browser bugs that were demonstrated to attack it. However, at the time of writing this chapter there is no published way to pirate games for the Switch.

SOLUTIONS AND RECOMMENDATIONS

These are common errors that were committed multiple times by multiple vendors.

Any single security mistake may be sufficient to break the security of any single console.

To create an efficient security system the manufacturer should perform a through code audit and ensure past mistakes are not present in the new product.

Security By Obscurity

Common mistake by all the vendors is to underestimate hackers' abilities. In the recent console generations hackers have reversed complex PowerPC code, tapped to the Xbox hyper-transport bus. Hackers resources, especially of modchip makers, should not be underestimated as there is prospering industry in attacking consoles security, especially for piracy.

Furthermore, contrary to common belief security by obscurity works at least partially. It appears that by reusing code from open-source or past projects the console becomes vulnerable to well-known attacks. Also, security by obscurity proved vital in protecting PS3, Xbox one and others.

Not Using Security Professionals

We have seen security mistakes in implementing cryptography by Microsoft, Sony and Nintendo. These security holes resulted in piracy in GameCube, PS3 and Xbox. These mistakes could have been avoided by hiring security experts to review the crypto code.

Community as Means to Reduce Piracy

Most modern consoles offer network-based gaming on their own private networks.

These networks force the users to upgrade to the recent operating systems and prevent downgrading to vulnerable system versions. As a result piracy rate immediately drop.

FUTURE RESEARCH DIRECTIONS

Today most consoles are already hacked. (with limited attacks against Xbox one and switch). Naturally unhacked consoles offer new challenges and interesting research area.

Creating a secure platform (Perhaps for generation 9 consoles) is another important research area.

However, the question of creating a trusted platform with decent DRM features for the mass market consumers has moved from consoles to mobile phones. Creating a phone that cannot be rooted and will create a trusted execution environment is a critical problem that Apple and Google are facing.

There is significant work and publications on rooting mobile phones as creating unbreakable versions. This research has many similarities to game console research as well as some additional challenges such as preserving battery life.

CONCLUSION

All modern game consoles security, except for the PS3 were broken (at least for offline piracy) in very short time. Broken security allowed game piracy hurting manufacturer revenues. We hope 9th generation consoles that will be released soon will pose greater challenge for hackers. We also hope console makers will enable Linux on the console and eliminate some of the motivation to attack the 9th generation consoles.

REFERENCES

- Anonymous. (2006). XBOX 360 hacked to run Linux. *26th Chaos Communication Congr.* Retrieved from <http://www.youtube.com/watch?v=4AGAhJuovY>
- Brown, M. R. (2003). *Playstation 2 independence day*. Retrieved from http://www.ifcaro.net/PS2_Independence_Exploit/original.htm
- Bushing, Sven, & Marcan. (2010). Console hacking 2010: PS3 epic fail. *27th Chaos Communication Congr.*
- Domke, F. (2006). Console hacking 2006. *23rd Chaos Communication Congr.*
- Domke, F., & Steil, M. (2007). Why Silicon-Based Security is still hard: Deconstructing XBOX 360 Security. *24th Chaos Communication Congr.*
- Domke, F., Steil, M., & Reilink, R. (2004). Game cube hacking *21st Chaos Communication Congr.*
- Lotz, Z. (2012). My whole life is a hack: how Geohot owned the iPhone, PS3 and inadvertently rallied hacktivists. *engadget*. Retrieved from <https://www.engadget.com/2012/05/01/new-yorker-profiles-geohot/>
- Marcan & Bushing. (2008). Console hacking 2008: Wii fail. *25th Chaos Communication Congr.*
- Mattrick, D. (2013). *Your feedback matters - Update on Xbox One*. Retrieved from <http://news.xbox.com/2013/06/update>
- Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417-426). Springer.
- Plutoo, Derreck, & Naehrwert. (2017). Console Security – Switch. *34th Chaos Communication Congr.*
- Steil, M. (2005). 17 mistakes Microsoft made in the Xbox security system. *22nd Chaos Communication Congr.*
- Stuart, K. (2013). Xbox One DRM restrictions dropped after gamer outcry. *The Guardian*.
- Sven, Marcan, & Comex. (2013). Console hacking 2013: WiiU. *30th Chaos Communication Congr.* Retrieved from http://media.ccc.de/browse/congress/2013/30C3_-_5290_-_en_-_saal_2_-_201312272030_-_console_hacking_2013_-_sven_-_marcan_-_nicholas_allegre_comex.html
- Takahashi, D. (2013). *Nintendo sold 2.4M wii-U consoles in 9 months. Less than Sony and Microsoft sold in 6 weeks*. Retrieved from <http://venturebeat.com/2014/01/29/nintendo-sold-2-4m-wii-u-consoles-in-9-months-less-than-sony-and-microsoft-sold-in-six-weeks/>

ADDITIONAL READING

Downing, S. (2010). Social control in a subculture of piracy. *The Journal of Criminal Justice and Popular Culture*, 14(1), 77–123.

Goodwin, S. (2013). Appliance Hacking: Converting Existing Technology. In *Smart Home Automation with Linux and Raspberry Pi* (pp. 53–86). Apress.

Nimmer, D. (1999). Riff on Fair Use in the Digital Millennium Copyright Act. *U. Pa. L. Rev.*, 148(3), 673. doi:10.2307/3312825

Resh, A., Kiperberg, M., Leon, R., & Zaidenberg, N. J. (2017). Preventing Execution of Unauthorized Native-Code Software. *International Journal of Digital Content Technology and its Applications*, 11.

Zaidenberg, N., Neittaanmäki, P., Kiperberg, M., & Resh, A. (2015). Trusted Computing and DRM. In *Cyber Security: Analytics, Technology and Automation* (pp. 205–212). Cham: Springer. doi:10.1007/978-3-319-18302-2_13

Zaidenberg, N. J. (2018). Hardware Rooted Security in Industry 4.0 Systems. *Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures*, 51, 135–151.

Zaidenberg, N. J., & Resh, A. (2015). Timing and side channel attacks. In *Cyber Security: Analytics, Technology and Automation* (pp. 183–194). Cham: Springer. doi:10.1007/978-3-319-18302-2_11

KEY TERMS AND DEFINITIONS

Boot Loader: A small piece of code that provides minimal functions. The boot loader is executed prior to booting the operating system. The boot loader typically provides minimal hardware drivers, file system support etc. that are required for reading the operating system code.

Chain of Trust: Group of computer components that starts at a trust nexus. Through a series of operations, each component in the chain adds functionality and verifies the next component. Thus, if the nexus can indeed be trusted then the final component can be trusted as well.

Console: An entertainment system designed to play video games (e.g., Microsoft's Xbox or Sony's PlayStation).

Data Execution Prevention (DEP or W^X): A paradigm that dictates that memory pages can have either execute or write permission but not both. Data execution prevention prevents self-modifying code and also attacks on the code that runs by itself (by exploiting buffer overflows and similar attack forcing the code to rewrite itself). DEP is a critical feature in almost all modern operating systems.

Digital Millennium Copyright Act (DMCA): A united state law that defines what constitute of fair use by the end-user and what constitutes as piracy or DRM violation. The DMCA criminalizes production of devices whose sole perhaps is breaking DRM.

Digital Rights Management (DRM): A software subsystem designed to allow rightful users to use contents (games, media) they paid for and disallow illegal use of contents the user has not paid for. DRM is mainly designed to limit the end-user, and as such, DRM software is not liked by the users.

Homebrew: Software that the end-user codes and/or compiles for his own (and his friends) device. This software is not suctioned by the device manufacturer who receives no royalties.

Hypervisor: Software package and hardware support for running multiple operating systems on the same hardware (e.g., VMWare ESXi, Microsoft Hyper-V, etc.).

Modchip: A hardware device that is soldered on top of existing product PCB replacing some chip. Usually, the modchip is designed to remove or disable the chip that handles copy protection.

Trusted Computing (Trusted Systems): Trusted systems are systems that are supposed to behave in a certain predefined way (for example, verify DRM). Local and remote software can attest that the system is indeed a trusted system before executing code.

Section 3

Drug Trafficking, Human Trafficking, and the Sexual Exploitation of Children

Drug Trafficking

3

Prabhjyot Kaur

University of Delhi, India

Puneet Kumar Kaushal

Lucideus Technologies, India

INTRODUCTION

Internet technology and its development have taken us to the next level of evolution (Dingledinel, Mathewson & Syverson, 2004). It has impacted almost every aspect of our lives. But it also has its own disadvantages such as enabling criminals to carry out their criminal operations in any corner of the world without being physically present (Sharma et al., 2018). Due to emergence of innovation in technologies, numerous ways have opened up for illegal trades, one of which is that of drugs.

It is a well-known fact that human beings have been using drugs since time immemorial, but the way they are used remains one of their most confusing behaviours (Evolutionary models of human drug use Wiki, n.d.). Though, fast rate proliferation of drug markets is taking place online with recent evidences suggesting the availability of any drug, they are the so-called cryptomarkets or the dark net markets that have been grabbing eyeballs for the guaranteed anonymity they provide to the users, be they sellers or buyers (Mounteney, Oteo & Griffiths, 2016). Researchers say, “There are now around 50 online market-places on the ‘dark web’ that trade illegal drugs, new psychoactive substances (NPS), prescription drugs and other – often illegal – goods and services” (Kristy, 2016). The internet has drastically changed the ways of doing business, including those of illegal markets.

Many organizations generate backend data that is dynamically retrieved through Web-form-based interfaces and thus not indexed by conventional search engines and this hidden, invisible, and unindexed content is called the Deep Web (Jung, Chun & Geller, 2008). The websites that form a part of the deep web cannot be accessed through the conventional search engines and requires specific software and configurations (Sharma et al., 2018). These sites contain the thoughts and ideas of many secret organizations, groups, and individuals who want to remain anonymous (Broséus et al., 2017). The dark web is a small portion of the deep web that is used mainly for illicit activities, because of the anonymity it offers it to its users (Mounteney, Oteo & Griffiths, 2016).

In order to venture into the deep web, a user will have to download a special browser which hides a website’s identity or IP, such as The Onion Router or TOR. As per the experts, “TOR encrypts web traffic in layers and bounces it through randomly-chosen computers around the world, each of which removes a single layer of encryption before passing the data on to its next hop in the network” (Greenberg, November 2014).

Cryptomarkets also involves financial aspects and thus, these markets also need to have some special forms of currency to provide a substantial level of anonymity. This is done by using cryptocurrencies such as Bitcoin (Cox, 2016). The present paper lays focus on this new means of acquiring illicit drugs from the markets available on the dark web, how these so called cryptomarkets have evolved through the use of technology to evade law and enforcement, their future and the role of governments in preventing this version of drug trafficking.

DOI: 10.4018/978-1-5225-9715-5.ch032

BACKGROUND

Drugs are defined as all substances and chemicals that should not be used for any purpose other than for medical and scientific research; if they are used for purposes other than these, they are called illicit drugs (Kassaye, 1999). Drugs are as old as human history and have been used for a variety of reasons in plethora of cultures; for religious purposes, for entertaining purposes, for altering the states of consciousness, as a matter of proud and for obtaining relief from pain, sadness and distress (Parmar et al., 2015). The black trading of drugs starts developing in jurisdictions where the law prohibits or restricts their sale (Drug trafficking, 2017). United Nations Office on Drugs and Crime defines drug trafficking to be a global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws (United Nations Office on Drugs and Crime, 2017). Several studies and researches have been conducted on the illegal trade of illicit drugs on the dark net. Martin gives a detailed description of the illegal drugs trade on the dark web, presenting the concepts of cryptomarkets and their commercial operations, analyses online and offline markets and discusses and suggests law enforcement practices (Martin, July 2017).

On the other hand, Buxton & Bingham explain that how the online drug trafficking reduces the scope of violence that occurs in traditional drug markets and how this approach can lead to dedication of resources towards more serious cybercrimes (Buxton & Bingham, 2015). Studies such as (Broséus et al., 2016), (Europol, November 2017), (Kruithof et al., 2018) and (Phelps and Watt, 2014) are area-specific, and analyse the situations in the respective regions. Some others analyse various cryptomarkets. Silk Road, the largest online drug market has been a topic of discussion in several papers (Aldridge & Décary-Héту, 2014; Barratt, 2014). The geographical analysis of Agora and Evolution has been performed in (Dolliver et al., 2018) and (Broséus, 2017) respectively. Cox talks about how feedbacks and ratings impact the reputation of the vendors on cryptomarkets (Cox, 2016). Aldridge and Décary-Héту have tried to project the future of the illicit drug markets (Aldridge et al., 2016). The same has been presented by Mounteney, Griffiths and Vandam (Mounteney, 2016). The market of illegal drugs, be they produced in laboratories or grown naturally, is gigantic and it is estimated that the annual global trade is worth \$321 billion (Drug trafficking, 2017).

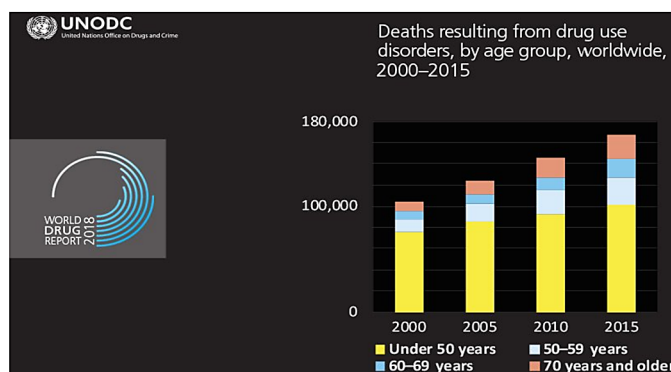
Today, majority of the countries in the world are getting trapped in the vicious circle of drug abuse and trafficking with the number of drug addicts increasing day by day due to many socio-economic reasons such as unemployment, poverty and socio-political disturbances (Parmar et al., 2015). Figure 1 shows the number of people by age, worldwide, as reported by the UNODC Report 2018 losing their lives due to drug use during the time period 2000-2015.

DARK WEB, DEEP WEB AND 'THE ONION ROUTER'

As per the experts, “searching on the internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep, and therefore, missed (Finklea, July 2017).” Thus, internet can be thought of as composed of two parts: one is the “Surface Web” and the other is the “Deep Web”. The Deep Web refers to “a class of content on the Internet that, for various technical reasons, is not indexed by search engines” (Finklea, July 2017). The dark web lies in the farthest corners of the deep one and is infamous for harbouring criminal and illegal activities such as trafficking of drugs, sex and humans, child pornography, sale of arms and weapons, sale of exotic animals and other illegal goods and services. The websites on dark

Figure 1. Deaths resulting from drug use disorders, by age group, worldwide, 2000-2015

Source: United Nations Office on Drugs and Crime (UNODC), World Drug Report 2018



web are intentionally hidden. At the same time, due to the privacy it offers, it is a hub for military, law enforcements, journalists, human rights activists, political leaders, reformers and many other organizations/individuals. Barratt further categorizes the content on deep web into five categories. (Barratt, 2018).

Onion routing was developed in the mid-1990s by three employees of the United States Naval Research Laboratory with the purpose of protecting the U.S. intelligence communications online and it was further developed by DARPA in 1997 (TOR (anonymity network) Wiki, 2018). The Onion Routing project, or Tor project was launched on 20 September 2002 (TOR (anonymity network) Wiki, 2018). As noted by the torproject.org, “The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor’s users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy” (The Tor Project Inc, 2017). Onion Routing is a distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell, and instant messaging wherein the users choose a path through the network and build a circuit, in which each node (or “onion router” or “OR”) in the path knows its predecessor and successor, but no other nodes in the circuit (Dingledine et al., 2004). The TOR network and the underlying TOR browser are based on Onion Routing. The TOR is an open source project and can be downloaded from the internet.

The use of TOR browser reduces the risk of what we call traffic analysis. Traffic analysis has been defined as “the process of intercepting and examining messages in order to deduce information from patterns in communication. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security” (Northcutt, May 2007). TOR also provides communications which are least prone to eavesdropping.

In the TOR network, relays are known as the computers that switch traffic from one computer to the other. There are around 7000 computers in the TOR network. All the relays run the TOR software, and this enables them to interact with every other relay (simply a computer) that is a part of the TOR network. So when any source wants to connect with a destination, a circuit is created. A circuit can be thought of as a path through which the traffic flows, right from the source to the destination. Every circuit in the TOR network lives for few minutes and after that it is pulled down and re-established by choosing a different set of relays. This is also known as virtual circuit. In this network, some computers or relays are special, and they are called as directory authorities. Their responsibility is to maintain a list of all possible relays at any given moment. The TOR browser then downloads this information and

builds a list of relays to choose from for communicating. The traffic flows through a minimum of three relays - the guard relay, the middle relay and the exit relay; each relay knows from which relay the traffic has arrived and to which relay it has to be sent but the complete circuit remains anonymous to each of the relays (Hassan, 2017).

The relays are publically listed in the TOR directory. As per (What is TOR?, n.d.), there are three types of relays - middle relays, exit relays and bridge relays. The first two relays are called the middle relays and play an important role in adding to the speed and robustness of the TOR network; they “advertise” themselves so that any other relay in the TOR network can connect to them. An exit relay is the one through which the traffic flows the last, before reaching its final destination and as they are second last in the circuit, are prone to being interpreted as the source of the data (What is TOR?, n.d.). Though relays are publicly listed in the TOR directory, there are some relays that are not. These are defined as “bridged relays”. In (What is TOR?, n.d.), they have been defined as “essential censorship-circumvention tools in countries that regularly block the IP addresses of all publicly listed TOR relays, such as China.”

In addition, TOR network also enables setting up of hidden services. This is the ability to anonymously host and browse content and services within a vast address space (Lewman, 2016). The first step is the installation of TOR and configuring the hidden service. Next, the hidden service has to advertise itself over the TOR network. For this, it randomly picks relays or so called ‘introduction points’ and establishes circuits with them. To receive connections, a hidden service descriptor is assembled which contains its public key and summary of each introduction point. Hidden service signs this with its own private key and it is uploaded on the directory servers. The descriptor will be found by clients requesting abc.onion where abc is 16 character name derived from its public key. Any client who wishes to contact the hidden service must know its onion address first. Then, the client downloads the descriptor from the directory authorities and gets to know about the public key and the set of ‘introduction points’. The client also picks a relay as ‘rendezvous point’ randomly and tells it one-time secret. When the descriptor is present and the rendezvous point is ready, the client prepares an introduce message containing the address of the rendezvous point and one-time secret and encrypts it with the public key of the hidden service. The client sends this to one of the introductory points which forwards it to the hidden service. Then, the hidden service decrypts it with its own private key and obtains its contents – the address of the rendezvous point and one-time secret. The hidden service creates a circuit to the rendezvous point and sends the one-time secret to it. Finally, the rendezvous point notifies the client of the successful connection establishment. The rendezvous point now simply forwards data between the client and the hidden service. A post by the TOR Project looks at the volume of hidden services traffic and estimates that there are around 30,000 active hidden services serving around 5 terabytes of information on a daily basis (Lewman, 2016). A sensational darknet marketplace that operated on TOR as a hidden service was Silk Road, created with a custom-generated domain name silkroad6ownowfk.onion.

SILK ROAD

Silk Road was founded in February 2011 by ‘Dread Pirate Roberts’ or DPR – a pseudonym that stood for either a person or a group of persons. Born in Austin, Texas, Ross Ulbricht is believed to be the man behind DPR and Silk Road. It was a haven for drug dealers, gun runners and document forgers and has been described as the internet’s Wild West and the eBay of vice (Norry, 2018).

Till its shut down by FBI in October 2013, Silk Road grew from an underground black market known by few, to a slick commercial enterprise that had been accessed by over a million people; it is estimated

that, in a little under three years, the site's users spent on a range of drugs: cannabis, prescription drugs, MDMA, LSD, heroin, crystal meth and every other illicit drug (Ormsby, 2016). All the communications were anonymized by the TOR browser, and the drugs were purchased online from vendors displaying eBay-style shop fronts and delivered through the post (Aldridge & Décary-Héту, 2014).

Researchers explain that 65% of the listings on Silk Road were related to the illicit drug trade which corresponded to around 13,000 listings for controlled substances, including opioids, precursors and stimulants while the other listings included 'services' mostly concerning computer-hacking; 'digital goods' such as pirated media content; and 'forgeries', predominantly fake identity documents (Hassan, 2017). Transactions used to take place in untraceable peer-to-peer cryptocurrency known as Bitcoin and the marketplace followed a strict system of escrow: payments weren't released to the vendors until the buyers were satisfied with the purchases. When Silk Road was shut down, FBI determined that over \$1.2 billion in sales had occurred involving 150,000 customers and 4000 vendors (Chertoff, 2017).

The Silk Road had always been characterized by the journalists, academicians and media as a resemblance to "business-to-customer" e-commerce platforms. But when some researchers downloaded 12000 listings on Silk Road together with profile pages of around 1000 vendors listing them, it was apparent that "many vendors were selling in quantities, at prices, and using terminology suggesting that they were knowingly selling to customers intent on resale: to customers who were themselves drug dealers" and arrived at the conclusion that "Silk Road was an online marketplace catering primarily to those making purchases for resale; that is, to street drug dealers buying stock to sell offline and to illegal drug manufacturers purchasing the products and services allowing them to synthesize illegal drugs" (Aldridge & Décary-Héту, 2014).

Some interviews conducted just after closure of Silk Road revealed that for some, the closure was a "catastrophe", for some it was "little more than temporal inconvenience", some had formed cordial relations with the vendors and carried out transactions through secured email bypassing the black markets altogether and others said they would return to the traditional methods of acquiring drugs (Ormsby, 2016).

But this crack down didn't stop the emergence of new cryptomarkets on the darknet throughout 2014. Just after 35 days when Silk Road was closed, Silk Road 2.0 came up and it was launched by the former Silk Road site owners. Several other darknet markets such as Pandora, Agora, Hydra, Evolution and Silk Road 2.0 competed with each other to win back the trust of the sellers and the buyers.

On 5 November 2014, 'Operation Onymous' was launched which as per Europol, was a joint initiative taken by the law enforcement and judicial agencies around the globe, coordinated by Europol's EC3, the FBI, ICE, HIS and Eurojust against "dark markets running as hidden services on the Tor network, aimed to stop the sale, distribution and promotion of illegal and harmful items which were sold on online dark marketplaces" as a result of which "410 hidden services taken down, 17 vendors and administrators arrested, and USD 1 million worth of Bitcoins, EUR 180,000 in cash, drugs, gold and silver seized (Europol, 2013)." Operation Onymous resulted in the closure of a number of cryptomarkets: Pandora, Silk Road 2.0, Black Market, Blue Sky, Tor Bazaar, Topix, Hydra, Cloud 9 and Alpaca (Europol, November 2017). The perpetrators didn't halt, again after 35 days of crack down of Silk Road 2.0, Silk Road 3.0 came up and is present on the dark net till now. There are still near about 14 marketplaces that appear to be operational and carrying out the black trade of illegal drugs: Valhalla, Dream Market, Silk Road 3.0, T•chka, Darknet Heroes League, Apple Market, House of Lions Market, TradeRoute, Wall Street Market, RSClub Market, Zion Market, Innite Market, CGMC and OW Market (Europol, November 2017).

THE ROLE OF CRYPTOCURRENCIES AND ENCRYPTION IN DARKNET MARKETS

Cryptocurrencies are used to carry out transactions on the Dark Web. These are decentralized and digital currencies that use anonymous, peer-to-peer transactions. For many years now, Bitcoin has been the primary facilitator of notorious drug transactions in the cryptomarkets. It allows anonymous buyers to pay the anonymous vendors in the absence of a proper, centralized financial system such as banks and is as difficult as TOR to be traced. Bitcoin is an “online virtual currency based on public key cryptography”, and was published in 2008 in a paper titled “Bitcoin: A peer-to-peer Electronic Cash System”, authored by someone behind the Satoshi Nakamoto pseudonym (Herrera-Joancomartí, 2014). As per bitcoin.org, “Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part” (Bitcoin, n.d.). Bitcoins are stored in “encrypted digital wallets” and are very difficult to be traced back once the transaction has been made (Chertoff, 2017). This happens because the transactions being made are though stored in a public ledger, only the addresses of the wallets and not the credentials of the persons owning them are stored. This ledger is called the blockchain.

Blockchain is equivalent to a bank statement, except it keeps track of the whole currency, rather than just an individual’s account (Cox, 2016). The blockchain is freely replicated and stored in different nodes of the bitcoin network, making it a completely distributed system (Herrera-Joancomartí, 2014). Blockchain also helps in mitigating “double spending problem” since it contains the history of all past transactions, where one can publicly see the amount of bitcoins or currency owned by each user.

Transactions can be thought of as lines in a double-entry bookkeeping ledger; each transaction contains one or more “inputs” which represent debits against a bitcoin account, there are one or more “outputs”, which are credits added to a bitcoin account and the outputs add up to slightly less than inputs as some small payment is collected by the miner who includes the transaction in the ledger (Antonopoulos, 2014). Blocks join together to give rise to blockchain and experts define a ‘block’ as a “series of updates of the transfers between addresses, as a fresh page in the ledger containing information about the block exactly preceding it” (Cox, 2016). A transaction is said to valid or successful if a block containing that transaction gets included in the blockchain.

There are two ways of obtaining bitcoins. One would be to buy them in exchange of traditional currencies by logging in to bitcoin exchange and other would be to ‘mine’ them. Adding a block to the blockchain is known as mining. Mining can be done by any user of the Bitcoin network using special software and hardware. Each block contains a tough mathematical problem that need to be solved before that block gets added into the Blockchain. So how is it done? “The mining process makes use of a proof-of-work system consisting of finding a hash of the new block with a value lower than a predefined target” (Herrera-Joancomartí, 2014). The miner who finds the solution for a block first is given some bitcoins as rewards. As mining is a very important part of the Blockchain system, miners also receive awards in the form of fees that each transaction pays to the miner. The role of public key cryptography in the Bitcoin system is presented below (Antonopoulos, 2014):

In Bitcoin, public key cryptography is used to generate a pair of keys, which control the access to Bitcoins. They are stored in the wallet of each user. This pair consists of a private key used to sign transactions to spend Bitcoins and a public key to receive Bitcoins. So in a way, these keys enable a user to prove the ownership of funds for transaction in the Bitcoin network, unlock the value to spend and transfer it to a new recipient. The private key is a randomly chosen 256-bit number and a one-way cryptographic function called elliptic curve multiplication is used to generate a public key. The Bitcoin address is also

generated from the public key using one-way cryptographic hash function. It is a string of digits and characters that can be shared with anyone who wants to send you money.

As per a *chainanalysis.com* report on the use of Bitcoins titled “Darknet markets are no longer a major use of Bitcoins”, it turns out that in 2017, more than \$660 million of Bitcoins were sent to the cyptomarkets and that is a more than 11-fold increase from the \$57 million sent to darknet markets in 2012, when the Silk Road, the first darknet market, was becoming popular (Chainalysis, 2018). At the same time it also reports that in March of 2012, nearly 30% of all Bitcoin transactions were being sent to darknet markets, but in 2017 this declined to less than 1% mainly because of three reasons, law enforcement closed the major darknet markets, Bitcoin became a financial asset, “crowding out its use as a means of illicit exchange” and new cryptocurrencies such as Monera, Zcash and Dash arose, providing greater anonymity and lower transaction fee.

Due to the illicit nature of the businesses conducted in the cryptomarkets, and to maintain anonymity, the administrators, buyers and vendors encrypt their communications using some encryption programme. Most commonly used one is PGP or “Pretty Good Privacy”. PGP was created in 1991 by Phil Zimmermann and is a computer programme that allows encryption of messages and files so that only the intended recipient is able to decrypt it and no third party can interpret the communication taking place between the two. PGP works as follows (Cox, 2016):

In this system, every user possesses two keys: a public key and a private key. These keys are files that could be stored on user’s computers. The public key is the one that is used to encrypt. Private key is used to decrypt. Private key must be kept secret ideally as it is used to decrypt any messages or files encrypted for a user, as well as signing any messages the user sends, to assure the recipient that they are indeed communicating with is the correct person. To use the encryption protocols, the user usually makes use of a special programme that has simple buttons such as ‘encrypt’, ‘save’ and others. The user types in the plaintext, chooses a public key that corresponds to the recipient, encrypts and finally sends it. Even if law enforcement agencies or the provider of email services intercept these messages, it is impossible to intercept the contents as long as the private key is not available.

DRUG TRAFFICKING ON DARK WEB

As already discussed, technology to maintain anonymity is being used to the fullest to commit illegal activities on the dark web. It is difficult for the law and enforcement to trace these activities. Billions of dollars are created by these businesses on the dark web and with passing days, they are flourishing. Several researches have been conducted on the kind of drugs being sold on the types of drugs being sold on the dark web websites. During 2016, the data and information collected and analysed by some researchers in aimed to focus on various aspects of the nature of drug trafficking on eight major cryptomarkets existing at that time, revealing that the number of transactions had tripled since the shut-down of Silk Road in 2013, revenues had doubled, listings placed by vendors played a major role to initiate the transactions, vendors from the USA dominated the cryptomarkets and the drugs which were sold the most were predominantly cannabis, followed by stimulants and ecstasy-type drugs (Kristy, 2016). As per the United Nations Report 2018, authorities in Europe has revealed some shocking statistics: “drug sales on the darknet from 22 November 2011 to 16 February 2015 amounted to roughly \$44 million per year but a later study estimated that, in early 2016, drug sales on the darknet were between \$14 million and \$25 million per month, equivalent to between \$170 million and \$300 million per year (United Nations

Office on Drugs and Crime, 2018).” Analysis of transactions done for various kinds of drugs done by Kruihof and others revealed some sort of stability, though, some changes were also observed (Table 1).

It was revealed that the rate of increase in vendor numbers across larger markets was consistent with Alphabay and Dream market being the largest of all the markets (Van Buskirk, 2016). It disclosed that in these two marketplaces, cannabis, pharmaceuticals, MDMA, cocaine and methamphetamine were the most famous and the popularity of NPS declining. In July 2017, major cryptomarkets Alphabay and Hansa, both TOR-based, were shut down. Alphabay was said to be ten times larger than Silk Road with around 250,000 listings on AlphaBay, 200,000 members and 40,000 vendors. On the other hand, Hansa had around 3,600 dealers who offered more than 24,000 drug product listings, from cocaine to MDMA to heroin (Greenberg, 2018). Several dark net markets still exist and are carrying the black trade of drug trafficking (Table 2). One an order is placed and payment to the vendor held in escrow, drugs are packed into vacuum seal packets and due care is taken to not leave any fingerprints or traces of DNA by dipping them in a bleach solution (Economist, 2017). The packets are labelled with printed labels and posted via far off post offices (Economist, 2017). According to criminologist James Martin, “reducing the violence of a bloody drugs war; promoting safer drug-taking practices through online forums; and supplying purer drugs, with fewer potentially deadly adulterants” are the major reasons behind the drug trade on the dark net (Martin, July 2017).

The extent to which users buy illegal drugs online can be analysed by numerous surveys conducted. Figure 2 shows the rise in number of drug users who had ordered drugs online in past 12 months, 2014-2017, clearly reflecting around 69% increase during this period.

Table 1. Number of transactions of various substances and their market share on the darknet, September 2013 – January 2016

Drug	Transactions September 2013	Transactions January 2016	Transactions in percentage: September 2013	Transactions in percentage: January 2016
Cannabis	10,663	30,790	31%	33%
Stimulants	4,898	17,206	14%	18%
Ecstasy-type	3,982	11,031	11%	12%
Prescription drugs	6,612	17,984	19%	19%
Opioids	2,015	5,241	6%	6%
Other drugs	735	465	2%	< 1%

Source: Kruihof, K., Aldridge, J., DécarvHéu, D., Sim, M., Dujso, E., and Hoorens, S., Internet-facilitated drugs trade (2018): An analysis of the size, scope and the role of the Netherlands. WODC, Ministerie van Veiligheids Justitie, 2016

Table 2. Drug listings in the major operating cryptomarkets

Name of the darknet market:	Onion URL:	Total Listings	Drug listings
Dream market	http://4buzlb3uhrjby2sb.onion	62,834	59,108
Wall Street	http://wallstyizjhkrvmj.onion	12,032	5,469
Point/Tochka Free Market	http://tochka3evlj3sxdv.onion	7,975	3,575
Silk Road 3.1	http://silkroad7rn2puhj.onion	51,829	31,633

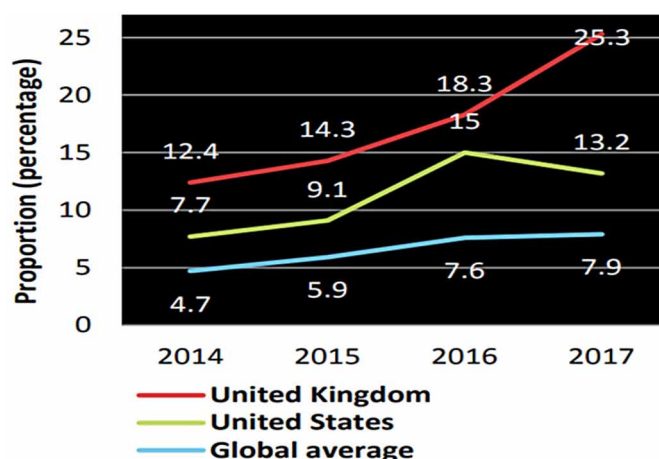
The results of an eleven-month long web crawling procedure implemented on daily basis by researchers on Silkkitie, the Finnish version of the Silk Road from November 2014 to September 2015 revealed in 2017 that the most famous drugs bought over this dark net market were stimulants and they were followed by cannabisproducts, empathogens such as MDMA and psychedelics (Nurmia et al.). Silkkitie was opened on 6th January on 2014 and was meant for purchase of sale and purchase of drugs in Finland only. This market facilitated smooth operations in Finland as there was no fear of being caught due to no security checks or screening anywhere. The extensive research over 93,878 observations of 260 sellers offering 3823 products. As with other markets, it also highlighted that higher were the positive feedbacks, higher were the sales, with the total sales of 41,131 items worth 171,387 Euros. As per Décary-Héty et al (2018), herbal cannabis, which is considered to be quite expensive in the USA, accounted for 21% of all sales observed on cryptomarkets, generating total revenue of US\$3.1 million per month. The customer discussions on a forum named drugs-forum.com revealed the sale of cocaine e-liquid in its free base form or crack cocaine freely available on dark web. Nichols (2018) says that Japanese drug dealers even offer free samples and give refunds if the customers are not happy with their purchases.

SOLUTIONS AND RECOMMENDATIONS

It is the need of the hour to devise policies to facilitate a more holistic approach in the detection and intervention of online drug trade. Numerous challenges are being faced by the law enforcement, such as, high resistance to take downs, crimes are committed in remote locations, the communications are encrypted, cryptocurrencies are used, presence of alternative banking platforms and utilization of cloud technologies (Phelps and Watt, 2014). Cox presents seven ways by which the police can track down anyone on the deep web, and these are, going underground, hacking, open source information, mass surveillance, digging through seized data, following the money and the postal system (Cox, January 2016). Hayes, Cappa and Cordon successfully tested a Web crawler using AppleScript for scraping dark web marketplaces that can be used to gather information about the numerous vendors and their listings on the dark web and can be of great importance for the investigators examining the criminal activity on it (Hayes et al., 2018). Michael Chertoff and Tobby Simon in (Koebler, February 2015) have

Figure 2. Annual drug users obtaining drugs over the darknet in the past 12 months, 2014-2017

Source: United Nations Office on Drugs and Crime (UNODC), World Drug Report 2017



devised some methods that can be used to scan the dark web. According to them, researchers should find “new ways to spot upcoming malicious [dark net] services to deal with new phenomena as quickly as possible.”According to them, monitoring customer data, hidden services and social sites, mapping the hidden services directory by operating the TOR network nodes, marketplace profiling and semantic analysis can aid in cracking anonymous nature of dark web and the illegal trades happening over it. It is the lack of correct knowledge, training and understanding of the deep web that serves as a barrier for the law enforcement to venture into the deep web and wage a war against them. The anonymity that deep web offers can be treated as an advantage rather, if they enact themselves as children, dealers or any other potential victims and start sitting in the chat rooms to monitor conversations (Lewman, 2016). De-anonymising the users of deep web and exploiting user mistakes will also aid in catching the criminals (Lewman, 2016). Economist recommends the law enforcement to continue the ongoing work against the major cryptomarkets emphasising on their administrators and moderators, find strategies to dismantle the trust existing between the vendors and the buyers and dismantle cryptocurrency that makes it possible to make and receive payments for drugs (Economist 2017). The existing scenario is a matter of big concern for the governments worldwide. Law enforcement is trying its best to curb this menace. The changing phase of the internet and technologies is enabling the criminals to go digital, and exploit nations’ resources. Continuous monitoring will be the best possible way to crack down the cryptomarkets. The governments and law enforcement authorities should train their agents to master the new technologies. If they would know the modus operandi of the cryptomarkets, they would know the methods to shut them down as well.

FUTURE RESEARCH DIRECTIONS

Only monitoring the websites that undertake drug trades is not going to be sufficient till the time we get to know that which type of substances are being used by whom. Drug user forums can be considered to be the rich sources of information, they themselves being online markets provide access to a large population of drug users than was available to the researchers earlier (Mounteney, 2016). It needs to be seen that how “balloon effect” happens, that is, how it has been a trend that when any market is taken down, new markets turn up in its place within so short periods of time. The postal systems are considered to be the fuel of these running engines. Though the buyers and vendors don’t ideally meet with each other in person, the postal systems deliver the drugs unknowingly to the buyers. Therefore, the role played here by post offices needs to be observed. The methodological issues regarding researching the deep web also widen the scope of research based on ethnography pertaining to drugs usage, sale and purchase accompanied with netnography and infodemiology (Mounteney, 2016). Tools and software need to be developed that can break the anonymity of the deep web. The role of social media needs to be analysed. Not only this, more clarity is needed as to why people move to online drug markets, what are the differences between the profiles of online vendors and the street dealers, how do quantities bought and sold on dark net actually look like and how do online markets interact with offline ones regarding the supply chain (European Commission Directorate-General Migration And Home Affairs, n.d.). The trade needs to be viewed and researched from every angle, starting from the growing relationships between vendors and buyers online, to delivery of the products and during the payment phase. Gwern Branwen, a researcher, web-crawled roughly 90 dark net places from December 2013 to July 2015 and gathered around 1.5 terabyte of data from 360,000 websites, “on the items sold, the Bitcoin price of the item, the date of the sale, shipping information, customer ratings and the vendor’s pseudonym” (Gwern et al., July 2015).

Not only this, Gwern in his studies also said the data set contains various vendor PGP keys, username (even clearnet names), and email addresses (Gwern et al., July 2015). Such researches in the future can be of great importance to shed some light on the deep web but as far as internet is concerned, the pace at which it is developing and evolving, it will always pose threat to the governments, law enforcements, research agencies and most importantly, mankind.

CONCLUSION

Internet has been a revolution in our lives. As it has got no geographical and international boundaries and can be accessed anywhere from the world, the number of internet users has increased drastically. This has led to increasing instances of severe cybercrimes. Cybercrimes have become extremely threatening and challenging crimes to be checked by the law and enforcement. Criminals are using the advancements in technology to their advantage. Mobile devices provide additional opportunities to carry out criminal operations while sitting in any corner of the world. It is difficult to nab the culprits as these crimes occur almost instantaneously and the enforcement agencies are ill-equipped and lack expertise. Various crimes such as identity theft, forgeries, child pornography, sex and human trafficking, terrorism and drug trafficking among others get efficiently planned and executed over a special and small part of the internet, called as dark web. It is indispensable to keep on researching and analysing both the dark web and deep web to keep an eye on the operations of the criminals and to allow adoption of new methodologies to reduce such malicious opportunities on the cyber space. As we have seen that drug trafficking has swiftly shifted from the streets to the cryptomarkets due to anonymizing browsers such as TOR, encryption, cryptocurrencies and increasing demand for illicit drugs, it becomes very important to shape laws and policies to combat this form of illegal trading on cyber platforms for the betterment of the society. In addition to this, international cooperation and coordination can play a major role in deploying these to tackle this internet facilitated drugs trade.

REFERENCES

- Aldridge, J., & Décary-Héту, D. (2014). *Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*. SSRN Electronic Journal.
- Aldridge, J., & Décary-Héту, D. (2016). Cryptomarkets and the future of illicit drug markets. *Insights*, 21, 23–29.
- Antonopoulos, A.M. (2014). *Mastering Bitcoin, Unlocking digital crypto-currencies*. O'Reilly Media, Inc.
- Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction (Abingdon, England)*, 109(5), 774–783. doi:10.1111/add.12470 PMID:24372954
- Barratt, M. J., & Maddox, A. (2018). Dark Web. *The SAGE Encyclopedia of the Internet*.
- Bitcoin. (n.d.). Retrieved from <https://bitcoin.org/en/>
- Breitbarth, A. K., Morgan, J., & Jones, A. L. (2018). E-cigarettes—An unintended illicit drug delivery system. *Drug and Alcohol Dependence*, 192, 98–111.

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International*, 264, 7-14. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0379073816300676>

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International*, 277, 88-102. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0379073817302037>

Buxton, J., & Bingham, T. (2015). The Rise and Challenge of Dark Net Drug Markets. *GDPO*.

Chainalysis. (2018). *The changing nature of cryptocrime*. Retrieved from https://www.chainalysis.com/static/Cryptocrime_Report_V2.pdf

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), 26-38. doi:10.1080/23738871.2017.1298643

Cox, J. (2016). Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets. *Insights*, 21, 49-54.

Cox, J. (2016). Staying in the shadows: the use of bitcoin and encryption in cryptomarkets. In *The Internet and drug markets* (pp. 41-47). Publications of the European Union.

Cox, J. (2016). *7 Ways the Cops Will Bust You on the Dark Web*. Retrieved from https://motherboard.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web

Décary-Hétu, D., Mousseau, V., & Vidal, S. (2018). Six Years Later: Analyzing Online Black Markets Involved in Herbal Cannabis Drug Dealing in the United States. *Contemporary Drug Problems*, 45(4), 366-381. doi:10.1177/0091450918797355

Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The Second-Generation Onion Router*. Retrieved from https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router

Dolliver, D. S., Ericson, S. P., & Love, K. L. (2018). A Geographic Analysis of Drug Trafficking Patterns on the TOR Network. *Geogr Rev*, 108(1), 45-68. doi:10.1111/gere.12241

Drug Trafficking. (2017). *New World Encyclopedia*. Retrieved from http://www.newworldencyclopedia.org/entry/Drug_trafficking

Economist. (2017). *Buying drugs online, Shedding light on the dark web*. Retrieved from <https://www.economist.com/international/2016/07/16/shedding-light-on-the-dark-webon>

European Commission Directorate-General Migration And Home Affairs. (n.d.). *Meeting report from the Internet and Drugs expert meeting*. Retrieved from https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/meeting_report_published.pdfon

Europol. (2013). *Press Release: Global Action Against Dark Markets On Tor Network*. Retrieved from: <https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-networkon>

Europol, Drugs, and the Darknet. (2017). *Perspectives for enforcement, research and policy*. EMCDDA, Europol.

Evolutionary models of human drug use Wiki. (n.d.). Retrieved on 1st December, 2018, from https://en.wikipedia.org/wiki/Evolutionary_models_of_human_drug_use

Finklea, K. (2017). *Dark Web*. Congressional Research Service. Retrieved from <https://fas.org/sgp/crs/misc/R44101.pdf>

Greenberg, A. (2018). *Operation Bayonet: Inside The Sting That Hijacked An Entire Dark Web Drug Market*. Retrieved from <https://www.wired.com/story/hansa-dutch-police-sting-operation/>

Greenberg, A. (2014). *Hacker Lexicon: What is the dark web?* Retrieved from <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>

Gwern, B. (2015). *Dark Net Market archives, 2011-2015*. Retrieved from <https://www.gwern.net/DNM-archives>

Hassan, Y. (2017). *The illicit drug trade on the dark net: Analysing the need for a new EU Framework*. Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/51952/MAThesis_Yasmine_Hassan_s1750283.pdf?sequence=1

Hayes, D., Cappa, F., & Cardon, J. (2018). A Framework for More Effective Dark Web Marketplace Investigations. *Information (Switzerland)*, 9, 186. doi:10.3390/info9080186

Herrera-Joancomartí, J. (2014). *Research and Challenges on Bitcoin Anonymity*. Springer International Publishing. doi:10.1007/978-3-319-17016-9_1

Jung, Y., Chun, S.A., & Geller, J. (2008). Toward the Semantic Deep Web. *Computer*, 95-97. doi:10.1109/MC.2008.402

Kassaye, M., Sherief, H. T., Fissehay, G., & Teklu, T. (1999). Drug use among High School Students in Addis Ababa and Butajira. *EJHD*, 13(2), 101-106.

Keefer, A., & Baiget, T. (2001). How it all began: A brief history of the Internet. *Vine*, 31(3), 90-95. doi:10.1108/03055720010804221

Koebler, J. (2015). *Six Ways Law Enforcement Monitors the Dark Web*. Retrieved from https://motherboard.vice.com/en_us/article/jp5a9g/six-ways-law-enforcement-monitors-the-dark-web

Kristy, K., Aldridge, J., DécaryHétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *The role of the 'dark web' in the trade of illicit drugs*. WODC, Ministerie van VeiligheidsJustitie, RB-9925-WODC. Retrieved from https://www.rand.org/pubs/research_briefs/RB9925.html

Kruithof, K., Aldridge, J., DécaryHétu, D., Sim, M., Dujso, E., & Hoorens, S. (2018). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. WODC, Ministerie van VeiligheidsJustitie.

Lewman, A. (2016). TOR and links with cryptomarkets. In *The Internet and drug markets* (pp. 33-39). Publications of the European Union.

Lightfoot, S. (2017). *Surveillance and privacy on the deep web*. Doi:10.13140/RG.2.2.21692.74889

Martin, J. (2014). *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*. London: Palgrave Macmillan. doi:10.1057/9781137399052

Martin, J. (2017). *Could The Dark Net Pave The Way Towards A Less Harmful Illicit Drug Trade?* Retrieved from https://www.huffingtonpost.com.au/2017/09/14/could-the-dark-net-pave-the-way-towards-a-less-harmful-illicit-drug-trade_a_23206913/

Mounteney, J., Griffiths, P., & Vandam, L. (2016). What is the future for internet drug markets? *Insights*, 21, 127-133.

Mounteney, J., Oteo, A., & Griffiths, P. (2016). The internet and drug markets: shining a light on these complex and dynamic systems. In *The Internet and drug markets* (pp. 13-17). Publications of the European Union.

Nichols, S. (2018). *Japanese dark-web drug dealers are so polite, they'll offer 'a refund' if you're not satisfied*. Retrieved from https://www.theregister.co.uk/2018/08/08/insights_asia_dark_web_report/on

Norden, S. (2013). *How the Internet has Changed the Face of Crime* (Unpublished Master's thesis). Retrieved from <http://fgcu.digital.flvc.org/islandora/object/fgcu%3A21423>

Norry, A. (2018). *The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin*. Retrieved from <https://blockonomi.com/history-of-silk-road/>

Northcutt, S. (2007). *Traffic Analysis*. SANS Technology Institute. Retrieved from <https://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis>

Nurmia, J., Kaskelab, T., Perälä, J., & Oksanen, A. (2017). Seller's reputation and capacity on the illicit drug markets: 11-month study on the Finnish version of the Silk Road. *Drug and Alcohol Dependence*, 178, 201-207.

Ormsby, E. (2016). Silk Road: insights from interviews with users and vendors. In *The Internet and drug markets* (pp. 33-39). Publications of the European Union.

Parmar, P., Rathod, G. B., Rathod, S., & Parikh, A. (2015). Drug Abuse and Illicit Drug Trafficking Vis-A-Vis Human Life – A Review. *Prensa Medica Argentina*, 101, 1. doi:10.4172/lpma.1000144

Phelps, A., & Watt, A. (2014). I shop online—recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation*, 11(4), 261–272. doi:10.1016/j.diin.2014.08.001

Sharma, S., Sharma, P., & Singh, G. (2018). Dark Web and Trading of Illegal Drugs. *J Forensic Science & Criminal Investigation*, 9(4), 555766. doi:0.19080/JFSCI.2018.09.555766

The Tor Project Inc. (2017). *Overview*. Retrieved from <https://www.torproject.org/about/overview.html.en>

TOR (anonymity network) Wiki. (2018). Retrieved 2nd December, 2018, from [https://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](https://en.wikipedia.org/wiki/Tor_(anonymity_network))

United Nations Office on Drugs and Crime. (2018). *Introduction*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_2_GLOBAL.pdf

United Nations Office on Drugs and Crime. (n.d.). *Global Overview Of Drug Demand And Supply, Latest trends, cross-cutting issues*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_2_GLOBAL.pdf

Van Buskirk, J., Naicker, S., Bruno, R., Burns, L., Breen, C. & Roxburgh, A. (2016). Drugs and the Internet. *Citation*, 2016(7).

What is TOR? (n.d.). Retrieved from <https://www.eff.org/torchallenge/what-is-tor.html>

ADDITIONAL READING

Godoy, G. A. S. (2015). *The drug trafficking inserted in cyber space - How social networks, virtual coins, big data and software applications influence it - An analysis of the United Nations organisation*. Interdisciplinary Insights on Fraud and Corruption.

Van Buskirk, J., Roxburgh, A., Farrell, M., & Burns, L. (2014). The closure of the Silk Road: What has this meant for online drug trading? *Addiction (Abingdon, England)*, 109(4), 517–518. doi:10.1111/add.12422 PMID:24397386

KEY TERMS AND DEFINITIONS

Block Chain: As the name suggests, block chain is a chain of blocks that serves as a public ledger of the Bitcoin network revealing ownership information of all the addresses. It is like a data file that contains the history of all the Bitcoin transactions that have taken place till now. Every block is based on its predecessor and contains information about the new transactions that got validated through it.

Cryptocurrency: It refers to any digital currency that uses certain encryption methods to secure and validate the transactions and generate new currency of its own kind.

Cryptomarkets: A cryptomarket may be defined as a platform for exchange of goods and services, both legal and illegal, on the dark web. They remain hidden from the world due to the use of anonymizing browsers such as TOR based on encryption techniques. Majority of the cryptomarkets undertake the sale and purchase of drugs.

Dark Web or Dark Net: Dark web can be defined as that miniscule portion of the deep web and hence the internet composed of websites whose IP addresses are intentionally hidden from the public using anonymizing tools such as TOR.

Drugs: A drug can be defined as any substance, chemical or natural, that is consumed for purposes other than medicinal and scientific.

Surface Web: It can be defined as that portion of the internet whose websites are indexed by search engines such as Google, Yahoo, and others. They are easily accessible and do not require the use of special software as needed for the deep web.

TOR: TOR or the onion router is free downloadable software that hides the IP addresses of the computers and hence lets its users protect their identity from traffic analysis.

Virtual Circuit: Virtual circuit is a path for the flow of data packets over a network, which does not exist in reality. It is 'virtual' in the sense that there is no dedicated physical layer link between the source and the destination of the data.

Domain-Specific Search Engines for Investigating Human Trafficking and Other Illicit Activities

Mayank Kejriwal

University of Southern California, USA

INTRODUCTION

Web advertising related to Human Trafficking (HT) activity has been on the rise in recent years (Szekely et al., 2015). Question answering over crawled sex advertisements to assist investigators in the real world is an important social problem. This problem involves many technical challenges (Kejriwal & Szekely, 2017c). This article will describe the problem of *domain-specific search (DSS)*, a specific set of technologies that can address these challenges. Modern DSS systems for investigative activities draw on cutting-edge techniques developed over three years of DARPA-funded research conducted in collaboratively academic (e.g., the University of Southern California's Information Sciences Institute), government (e.g., NASA's Jet Propulsion Laboratory) and industrial (e.g., Uncharted) settings. Evidence from the HT domain shows that the systems can be used to provide valuable utility to analysts and investigative experts.

In illicit domains such as HT but also others like securities fraud and narcotics, domain-specific search involves a form of *Information Retrieval (IR)* that takes as input a large *domain-specific* corpus of pages crawled from the Web. The system allows investigators to satisfy their information needs by posing *sophisticated queries* to a special-purpose engine. A workflow of this process is shown in Figure 1. Since investigators are largely non-technical, they must be able to issue such queries to (and receive responses from) intuitive, graphical interfaces. A fully functional DSS engine must have some notion of semantics, since sophisticated queries go beyond just keyword specification. This is because investigative queries are more like real-world questions requiring complex operations like aggregations (e.g., *find me all email addresses linked to the phone 123-456*).

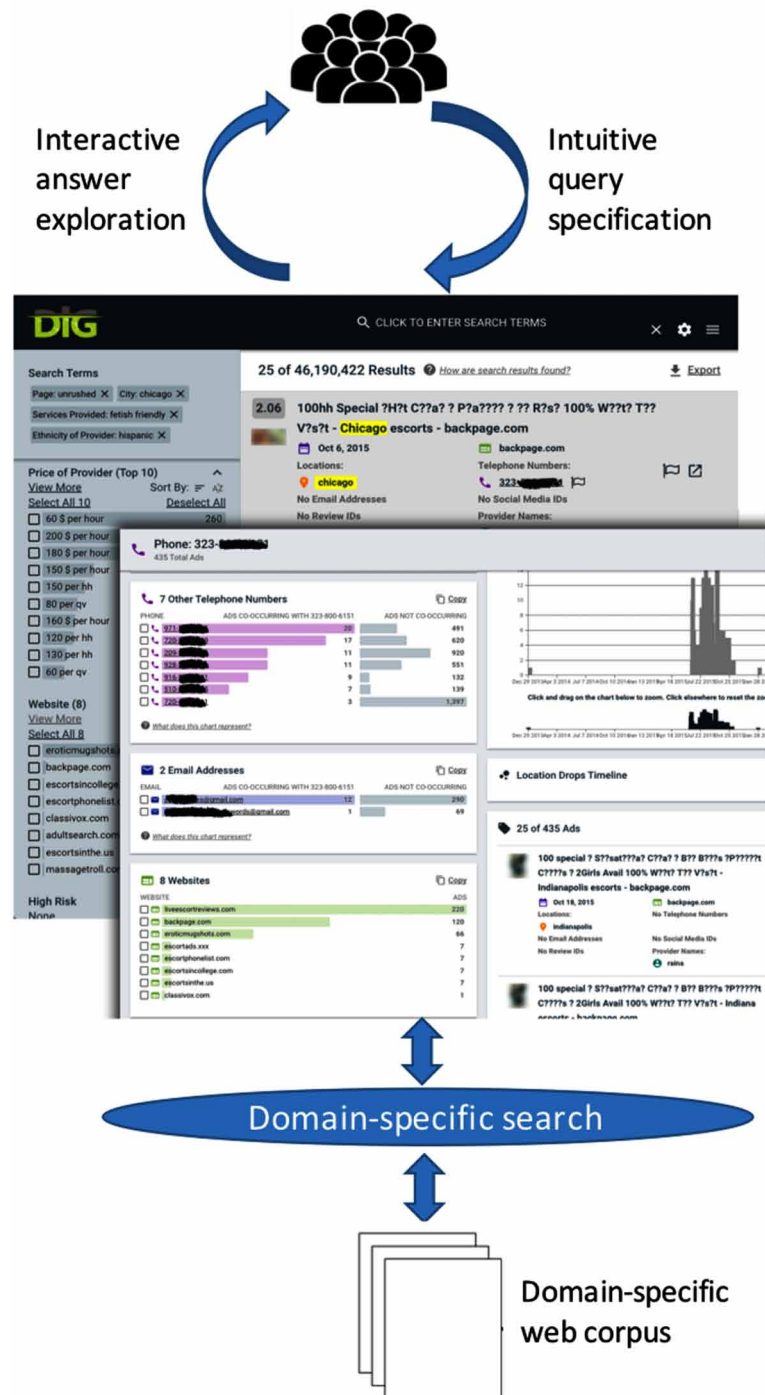
A viable solution to the problem has to allow the user to pose queries both intuitively and interactively.

For such a DSS to operate semi-automatically and be useful in the real world, several challenges and desiderata must be fulfilled. Possibly the most important of these is handling the unusual nature of an illicit domain, since investigators who have to use the system have special needs. To understand why this can be challenging, consider the recent advent of technologies like neural networks and deep learning. Pre-trained tools such as word embeddings and Named Entity Recognizers in the natural language processing community have also been released for public use (Pennington, Socher & Manning, 2014). However, many of these tools have been trained on datasets and corpora that are fairly 'regular' i.e. comprise of relatively well-structured text (like news corpora and Wikipedia articles). Consequently, they are not necessarily suitable for language or data acquired in illicit domains. Table 1 illustrates some examples of real text scraped from sex advertisement webpages (but with identifying phone numbers appropriately modified). Acquiring and labeling data from such domains is both expensive and sensitive,

DOI: 10.4018/978-1-5225-9715-5.ch033

Figure 1. A procedural workflow of domain-specific search from the point of view of an investigative user, using the domain-specific insight graph (DIG) DSS for example interfaces

3



not easily amenable to crowdsourcing (Kejriwal & Szekely, 2017a). A purely machine learning-based approach is simply not feasible.

Furthermore, the challenge of building a DSS is compounded by the fact that many of the component Artificial Intelligence (AI) tools and methodologies still haven't come close to achieving high-quality human-level performance. These tools span areas like NLP and Semantic Web, and in a real-world architecture, need to operate in tandem. In unusual domains with irregularities, noise is inevitable at every stage of the process and has to be dealt with, rather than assumed away, in the design of the architecture itself. This requires multiple measures of robustness, and a careful understanding of what kinds of noise the end-user (investigators) would find acceptable. Imprecise or careless design can lead to the problem of cascading errors, making a full system unusable.

Over years of careful research funded under the DARPA Memex program, an end-to-end architectural framework has been developed as an admissible and principled way of building an end-to-end DSS for illicit domains, with particular emphasis on human trafficking. One instantiation of the architectural solution, available as both open source code and executable in a stand-alone Docker container, is the *domain-specific insight graph* or DIG system that was built at USC ISI. DIG was rigorously evaluated on real-world data collected from over 90,000 sex-advertising webpages collected over the first half of 2016 (Kejriwal, Szekely & Knoblock, 2018). The principles behind DIG have been replicated independently by an industrial team. Along with other DARPA projects, DIG has been used to prosecute traffickers in the US, and to rescue trafficking victims. Recently, an engine of this type was being used by over 200 law enforcement officials to fight the overall problem of sex trafficking and related illicit activities.

This encyclopedic article will describe the background, main principles and challenges of building a DSS in illicit domains, with a strong focus on human trafficking promoted through illicit sex advertisements on the Open Web. The article will conclude with a description of promising avenues for future research.

BACKGROUND

Building domain-specific search engines for non-traditional domains requires synergies across a range of areas, knowledge graph construction (KGC), machine learning and analytics (especially using intuitive interfaces), and information retrieval (IR). Although a complete review of these fields is beyond the scope of this article, we synthesize core elements below.

Table 1. Example fragments of text extracted from real-world illicit sex advertisements. Note that identifying information has been replaced. Information that is potentially useful to investigators and/or to a semantics-aware domain-specific search engine is highlighted in bold.

Italian 19 hello guys...My name is charlotte , New to town from kansas
[GORGIOUS BLONDE beauty] ? FROM Florida ? (Petite) ? [CURVY]?
NO DISAPPOINTMENTS. 34C.. Brazilian,ITALIAN beauty...
Hey gentleman im Newyork and i'm looking for generous
Hi guy's this is sexy newyork .& ready to party.
AVAILABLE NOW! ?? – (1 two 1) six 5 six – 0 9 one 2-21

Information Integration (II)

Information integration, also commonly known as *data* integration, is generally defined as the problem of providing a unified query interface over multiple data sources (Lenzerini, 2002). Information integration has been a research subject for at least 40 years (El-Masri & Wiederhold, 1979); recent developments and foundational principles are synthesized in the book by Doan et al. (2012). The problem has gained importance with the advent of Big Data (Dong & Srivastava, 2013), in domains ranging from enterprise to computational biology and Web search (Gupta et al., 2013; Brambilla, Ceri & Halevy, 2013; Gomez-Cabrero et al., 2014; Loshin, 2013). Despite the enormous progress in information integration over the last few decades, there are some key challenges in the HT domain that preclude a direct adaptation of many existing techniques. These challenges will be described later in the article.

Information Extraction (IE)

Information extraction is a core component of any information integration and Knowledge Graph Construction (KGC) pipeline over Web corpora, as the unstructured webpages must first be structured in order for fine-grained queries to be executed over them. With the initial advent of the Web, wrapper induction systems had proved successful for several IE domains (Kushmerick, Weld & Doorenbos, 1997). Influential work in the early 2000s e.g., STALKER (Muslea, Minton & Knoblock, 2003) used machine learning methods for the wrapper induction problem (Lerman, Minton & Knoblock, 2003). Such methods were inherently data-driven, and were less brittle than rule-based wrapper architectures. More recent Web information extraction systems include the approach by Barrio and Gravano (2017), and Martinez-Rodriguez, Hogan and Lopez-Arevalo (2018).

IE systems have continued to evolve since then; Chang et al. (2006) provide a comparative survey of many of the leading IE techniques along three dimensions (task domain, degree of automation and the actual techniques used), a key finding being the dependence of techniques on the actual input format. More recently, deep learning and other modern machine learning methods have been applied to domain-specific IE, in domains as diverse as cancer pathology, healthcare and social manufacturing (Qiu et al., 2018; Leng and Jiang, 2016)

More recently, OpenIE has become a popular topic of research, owing to the need for IE techniques that do not rely on pre-specified vocabularies (Etzioni, Banko, Soderland & Weld, 2008), but this work is largely orthogonal to advances in DSS, since the vocabulary and domain have to be specified. For more recent advances in Open IE, we refer the interested reader to the work by Bhutani, Jagadish and Radev (2016), Angeli, Premkumar and Manning (2015), and (in the case of multilingual IE), Gamallo and Garcia (2015).

Search and Knowledge Graphs

The kind of structured querying described in this article is more broadly known in the literature as *entity-centric search*, defined by Dalvi et al. (2009) as creating a ‘semantically rich aggregate view’ of concept instances on the Web. Entity-centric search has led to novel insights about the search process itself, two examples being knowledge base acceleration and filtering (Frank et al., 2012), and interactive search and visualization as in the Timemachine system (Saleiro, Teixeira, Soares & Oliveira, 2016). More recent work on entity-centric search includes the work by Kejriwal and Szekely (2017b), Querytogether (Andolina et al., 2018), Deeplife (Ernst et al., 2016) and InfoScout (McKeown et al., 2016). The

patents filed by Pantel et al. (2017) and Roberts et al. (2016) are also relevant, especially for insights in the industrial space.

While interactive search and visualization is particularly relevant to the present work, many established search systems are designed to keyword-only queries rather than for the kinds of aggregation and dossier generation queries (subsequently described) that are so fundamental for robust DSS. This also distinguishes the concepts described in this article from other similar research that fuses Semantic Web research with IR research on tasks such as ad-hoc object retrieval (Freitas et al., 2012; Tonon, Demartini & Cudre-Mauroux, 2012). Despite the differences, important elements of the DSS described herein are inspired by the hybrid (instead of purely structured or unstructured) search techniques used for entity-centric search tasks in these systems.

In more recent years, entity-centric search has been used in commercial search engines like Google. For example, keyword searches like ‘Albert Einstein’ are now treated by Google both as keyword and as entity-centric search. For facilitating the latter, Google uses its underlying Google Knowledge Graph technology, based on a proprietary version of the (previously open-source) Freebase knowledge base (Bollacker et al., 2008; Singhal, 2012). However, the query medium is still largely keyword based, unlike the complex queries that illicit-domain DSS systems can handle. Another extremely important difference is that illicit domains like human trafficking exhibit a *long-tail* distribution (Kejriwal & Szekely, 2017b) that is uncharacteristic of entities in the Google Knowledge Graph, which largely contains world knowledge from a handful of sources such as Wikipedia and Wordnet (Gabrilovich & Markovitch, 2007; Miller, 1995). More recently, schema.org and markups have started to play an important role in populating the Google Knowledge Graph (Paulheim, 2017; Nam & Kejriwal, 2018).

Human Trafficking

One of the most important aspects of this article is its focus on a non-traditional domain that has an outsize presence on the Web, and by some estimates is a multi-billion dollar industry, but due to technical and social reasons, has largely been ignored by the computational, knowledge management and IR research communities till quite recently (Hultgren, Jennex, Persano & Ornatowski, 2016; Alviri, Shakarian & Snyder, 2016). An exception, and a prime focus of this article, is the DIG (Domain Insight Graphs) system. Similar to the DeepDive system (Niu et al., 2012), which also makes knowledge graph construction intuitive, DIG implements KGC components, includes a GUI, and was evaluated on human trafficking data (Kejriwal & Szekely, 2017b).

More broadly, semi-supervised and minimally supervised AI has been applied to fight human trafficking in contexts beyond information extraction and search (Kejriwal et al., 2013; Rabbany, Bayani & Dubrawski, 2018; Alviri, Shakarian & Snyder, 2017; Burbano & Hernandez-Alvarez, 2017). As one example, the FlagIt system (Kejriwal et al., 2013) attempts to semi-automatically mine *indicators* of human trafficking, including movement, advertisement of multiple girls etc. As another example, Rabbany et al. (2018) explore methods for active search of connections in order to build cases and combat human trafficking. Finally, although this article deals primarily with linguistic data (since it is focused on IE, which tends to work on linguistic data), there has also been a steady stream of work on the non-linguistic characteristics of sex ads. For example, recently, Whitney et al. (2018) describe how emojis can be used to add a layer of obfuscation to sex ads to avoid getting investigated, caught and prosecuted. Even if investigators invested the effort to painstakingly construct ground-truths, the creative and dynamic ways in which traffickers adapt (e.g., by using obfuscations such as emojis and misspellings)

would soon render those ground-truths stale and obsolete. Hence, there is a real need for developing end-to-end unsupervised IE systems, both for acquiring and evaluating extractions.

Finally, although this article is mainly concerned with building DSS engines for human trafficking, we believe that the core findings apply to other illicit domains e.g., from the Dark Web (Chen, 2011), that are highly heterogeneous, dynamic and prone to deliberately obfuscate key information like phones (Table 1).

FOCUS OF THE ARTICLE

This section introduces the problem of domain-specific search (DSS), especially in the context of fighting illicit activity (sex advertising activity is used as the primary example) with an online footprint, and the challenges that successful DSS must overcome to adequately solve this problem. Solutions and recommendations will be described in the next section.

The field of online search, as it exists today, has been largely researched under the banner of information retrieval (IR). The majority of IR research has tended to focus on generic search and generic users, embodied by search engines like Google and Bing. According to Yan, Song and Li (2006), domain-specific IR has become more popular in the last decade since ‘not only domain experts, but also average (i.e. non-expert) users are interested in searching domain specific information from online resources’. Although their work was primarily in the health and medical area, and the IR they are referring to is still *document-centric*, the key motivation (making such technology accessible to non-experts) has become ever more important in an age when machine learning and other models have become complicated to set up. In illicit domains, where the primary users are law enforcement and people who do their investigative work ‘on the ground’, it is ever more important to make domain-specific search technology accessible, relatively complete and trustworthy, and easy to use.

Furthermore, one could reasonably argue that, the more complex the domain, the more sophisticated the needed IR facilities. To distinguish the traditional definition of ‘domain-specific IR’, which has involved corpora of domain-specific definitions, this article refers to the problem of satisfying investigators’ needs in a domain such as online sex commerce as domain-specific *search*. In the context of this article, domain-specific IR involves a subset of DSS. In the simplest case, an investigator could enter a search lead, such as a phone number, or some keywords (e.g., describing the physical attributes or last known location of a victim), and expect an IR-like solution where a *ranked* list of relevant advertisements (hopefully containing not just the keyword query but also additional details that the investigator can use to search *further*) appear. The utility of such *point fact* queries¹, while necessary, is hardly sufficient. Generally, investigators want more detailed information, including aggregations. For example, the investigator may want to enter the phone number and expect the system to *know* that the number is a phone number, and show her *all available* information (a ‘dossier’ capturing global information) on that phone number (including activity timelines, counts of ads the phone has appeared in, associated email addresses etc.). In other words, the system should not only have some notion of *semantics*, but should be capable of *global* rather than *local* processing of retrieved answers. We provide examples of some of these query types from the HT domain in Table 2.

In fact, a truly robust DSS system should be able to accept hybrid questions that are a combination of point fact, aggregation and the *dossier generation* query mentioned above informally. An example of such a question from the human trafficking domain is *Return a time series of activities of phone numbers associated with the following information set: Name: Candie, Location: Los Angeles, Services Adver-*

Table 2. Real-world examples of the different structured question categories in the human trafficking domain (identifying information has been masked). Many of these query categories have also been found to apply to investigative IR tasks in other illicit domains, including penny stock fraud.

Query category	Example
Point fact	Find names of escorts associated with phone number 123-456-9999 who are older than 23
Cluster identification	List all ads connected via a shared email address to the email XXX@Z.org
Cluster facet	List all ads connected via a shared phone number or email to the phone number 1234400 that optionally feature the phrase ‘Maria funsize’ in the description
Cluster aggregate	Find most common ethnicity of escorts associated directly with phone number 123-456-9999

tised: *Massage, Nuru*. The point fact aspect of the query arises from the information set specified, while aggregation is required because the user has asked for all phone numbers associated with the information set. Finally, the activity time series of each of these phone numbers can only be obtained from the dossier compiled on that phone number.

Note that, for higher accuracy, the user would actually specify such questions using *forms* or structured queries so that user intent is not misinterpreted by the system. Figure 2 illustrates the query interface for the DIG DSS instantiated for the human trafficking domain with some fields filled in. The query is now not just a ‘bag of words’ but contains words with semantics (since they are specified for fields like Product and Email) and can be further enriched using disjunctions (by using comma between terms) and conjunctions (by clicking on the star symbol next to the field so that it turns from blue to yellow).

The query that emerges as a result of such inputs is reminiscent of an SQL or SPARQL query prevalent in the database (and for SPARQL, Semantic Web) community. Even there, one must be careful. Executing the query ‘as is’ is often problematic because of the *noise* in AI modules (like information extraction; see also the challenges subsequently enumerated) alluded to in the introduction. For example,

Figure 2. The DIG DSS search form (‘query interface’) for the human trafficking domain that allows users to pose semantically-enriched queries

considering the query above, there may be some ads where Candie's location is 'LA' rather than 'Los Angeles'. In other ads, Candie's name may be misspelled, but the rest of the context in the ad may still make it evident that the person is the same. To handle such cases, *query reformulation* is required. That is, the constraints and inputs in the original query must be modified to 'capture' such cases without introducing too much noise, so that aggregation and dossier generation results are not overly conservative.

Building DSSs that can generalize in the ways described above, in illicit domains, is a challenging problem, especially with limited resources. Table 3 briefly lists and describes some of these challenges. In normal cases, to maintain good quality and coverage, an investigative customer would have no choice but to hire a technical team to understand their needs and construct a DSS over months or years of effort. This is out of reach for resource-strapped investigative agencies in most countries. The DARPA Memex program, mentioned earlier, was a 4-year program that attempted to democratize the *construction* and *use* of powerful DSS technology by non-technical investigators². Use of such engines, once constructed, could be accomplished through an intuitive Graphical User Interface (GUI) and some training, but construction required creativity, since it is traditionally the domain of technical experts. The technologies and architecture that resulted from years of research on Memex are described in the next section.

SOLUTIONS AND RECOMMENDATIONS

Given the problem definition of DSS as described in the previous section, and the numerous, formidable challenges that successful DSS must overcome, what should a good solution 'look' like? This section describes an *architectural* solution that has been instantiated and developed over the course of the DARPA Memex program and transitioned to, and tried by, multiple law enforcement agencies in the United States

Table 3. A non-exhaustive set of challenges that an illicit-domain DSS must generally overcome to be useful to real-world investigators

Heterogeneity of webpage structure , making wrapper induction difficult to automate with sufficient quality. In the human trafficking domain, many sex ad portals have to be crawled, which makes generalization and manual training too infeasible
Non-traditional nature of domain, including linguistic patterns (see Table 1 for examples from the human trafficking domain) and types of fields in the domain ontology; e.g., uncommon fields like stock ticker symbols have to be extracted for the penny stock fraud domain, while physical attributes, phones, locations and sex services provided have to be extracted for HT
Scale and infrastructure , since a truly comprehensive DSS must involve sophisticated query execution over domain-specific corpora crawled at Web-scale
Robustness to potentially irrelevant content both in the corpus and within webpages; for example, in the human trafficking domain, webpages on backpage.com and other portals often feature sponsored ads that can be difficult to automatically ignore
Presence of missing values and noise , due to both information obfuscation (see below) and due to imperfection in the AI systems for extracting key attributes; e.g., due to creative writing of phone numbers in the human trafficking domain, and conflation with other numeric attributes like age (last row of Table 1)
Robustness to information obfuscation , since illicit players are often trying to evade investigative search by creatively masking identifying information (examples from the human trafficking domain of both obfuscated phones and names are shown in Table 1)
Complex query types , since, as Table 2 described for the human trafficking domain, domain-specific search for investigative IR involves operations like aggregation and dossier generation, in addition to the point-fact style queries of traditional IR engines
Preclusion of live Web search , due to the dynamic nature of illicit domains where webpages are frequently taken down and possibly 're-posted', sometimes with different pictures and locations. To answer questions involving time series, for example, pages have to be <i>cached</i> , which makes scale even more of a challenge. In the human trafficking domain, such pages have also been used for evidence gathering (as the Memex tools have been used in various documented prosecutions).

to fight human trafficking. While covering the full technical breadth of the solution is beyond the scope of this article, key details and design decisions are described, with pointers to further reading.

The architectural overview of the DSS developed under Memex is illustrated in Figure 3. As a first step, the system attempts to discover relevant websites in the user's *domain of intent* through a process that goes alternately by the name of *domain discovery* or *intelligent crawling*. In the literature, the latter term is more prevalent, having been researched under various settings (Aggarwal, Al-Garawi & Yu, 2001), but more recently, the former term has also started becoming popular (Krishnamurthy, Pham, Santos & Freire, 2016). The idea is to (iteratively) accept as input, various intuitive cues describing the domain such as keywords and websites, and find *relevant* webpages on the Open Web that seem to conform to the definition of the domain. For example, in the human trafficking domain, seed keywords would include terms such as 'escort' and 'massage parlor' and a seed website might be 'backpage.com'. Concerning relevance determinations, one could use classic techniques (such as a pre-trained learning-to-rank classifier) but over the course of the Memex program, methods employing reinforcement learning and lower-supervision machine learning paradigms have also been explored with success. A good example of a system implementing many of these techniques and also offering an intuitive interface to the user who is attempting to provide seeds and define the domain, is ACHE, developed by a group at New York University (Krishnamurthy et al., 2016).

The second step, which is much more challenging and can determine the quality (especially, *precision*) of the system and its outputs as a whole, is *knowledge graph construction (KGC)*. KGC encompasses a set of roughly sequential techniques (see Background for related work and references), such as information extraction, entity resolution and advanced knowledge graph identification techniques such as knowledge graph embeddings. All of these techniques are designed to operate in tandem to ingest a corpus of raw data (usually, natural language documents or 'semi-structured' webpages) as input and to output a *knowledge graph (KG)*, which is defined as a directed, labeled multi-relational graph expressing entities (labeled nodes) and relationships between entities (labeled edges).

Among these steps, Information Extraction (IE) is a well-studied area in both the natural language processing and Web communities (Chang et al., 2006). Except for the problem of *Open IE*, almost all

Figure 3. An architectural overview of the DSS developed under the DARPA Memex program, particularly for human trafficking

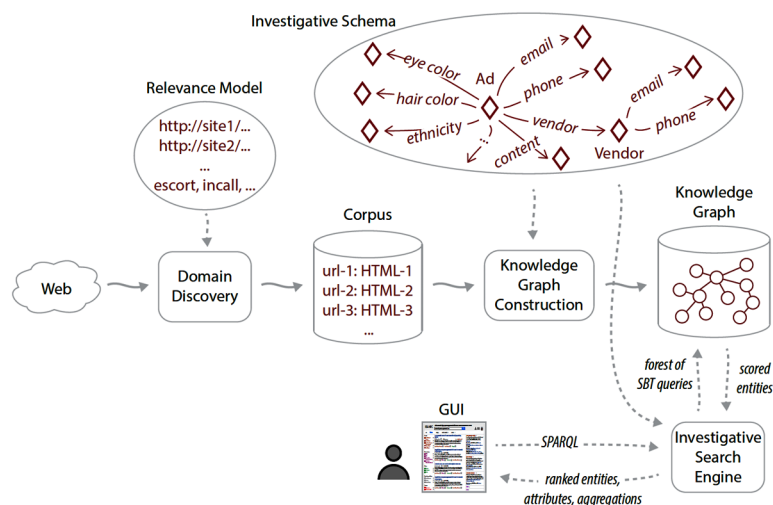
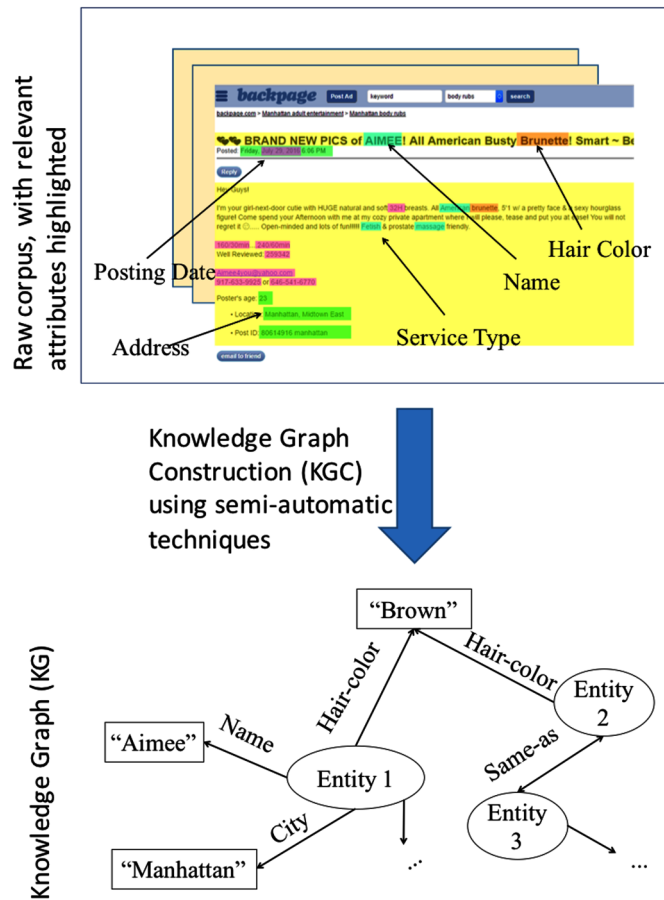


Figure 4. A brief illustration of knowledge graph construction (KGC) wherein relevant attributes (specified according to a domain-specific investigative schema) are semi-automatically extracted and resolved into a directed, labeled multi-relational KG



other forms of IE are *ontology-based*. That is, an underlying ontology, which could be as simple as a set of terms (e.g., PERSON, LOCATION and ORGANIZATION) or a complex event ontology such as ACE, which ontologizes events ranging from interaction to movement and destruction, including attacks (Doddington et al., 2004). In the case of illicit domains, the ontology in terms of which IE is performed is referred to as an *investigative schema*. A real fragment of the investigative schema developed by experts for investigating human trafficking is shown at the top of Figure 3, and includes both physical attributes, as well as identifying attributes such as phone number.

Following IE, steps such as Entity Resolution (ER) can be undertaken to clean up the KG even further (Getoor & Machanavajjhala, 2012). Again, in illicit domains, one should always attempt to customize the ER algorithm to achieve higher performance. For example, phones tend to be highly obfuscated in sex advertisements, making it likely that phone extractions have noise that obeys certain characteristics (e.g., extra digits, presence of the + symbol or extra 0s etc.). ER can be customized to take these cues into account to achieve higher precision or recall. Other advanced techniques like knowledge graph embeddings are also applicable. The reader is referred to a survey on knowledge graph refinement for full details on these procedures (Paulheim, 2017).

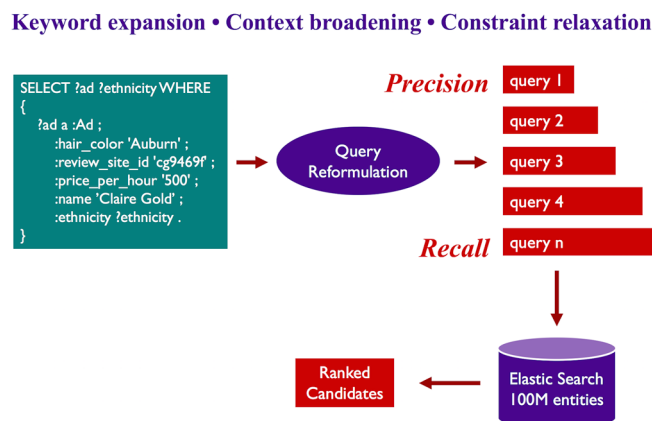
Ultimately, the end result of knowledge graph construction (and optionally, but recommended, refinement) is a knowledge graph. This knowledge graph can be queried in a structured language, using intuitive interfaces like forms, options and even free-text. However, the KG will be noisy, despite application of advanced KGC and refinement, and the query may not always fully express user intent. Thus, query reformulation is an important recommended step that must be used for good performance. In experiments conducted under the Memex program, even simple query reformulation was found to be necessary to achieve non-zero performance on query retrieval metrics like Mean Reciprocal Rank (Kejriwal & Szekely, 2017b).

The original query, which would usually be expressed using a form such as in Figure 2, is (approximately) rendered in SPARQL. The strength of a reformulated query's weight is generally inversely related to the amount of reformulation compared to the original query. The query is from the HT domain.

An intuitive visual description of query reformulation is given in Figure 5. As the figure shows, a query can be reformulated using a variety of well-researched techniques (keyword expansion, constraint relaxation and context broadening) designed to expand the coverage of the query. The simplest of these techniques is keyword expansion, which involves *supplementing* the original words with *related* words to help improve search recall. As an intuitive example of keyword expansion, one could replace an instance of a 'sub-type' ethnicity like 'Japanese' with a super-type ethnicity like 'Asian', or a color like 'auburn' with the synonym 'red'. Another example technique is constraint relaxation, which involves turning some of the query specifications into *optionals* so that not every criterion has to be successfully met for a result to be retrieved. This can especially help with misspellings, difficult-to-extract attributes or unusual synonyms.

In practice, the more aggressive query reformulation is, the more precision can suffer. This may help the system to retrieve some more relevant results, but it will also bring irrelevant ads into the fold. Similarly, instead of looking for 'Japanese' in the ethnicity field, the query could be relaxed to search against the entire text. This improves recall but can also backfire. The trick is to leverage the global power of the system by compiling the final set of results through combining individual query results. NoSQL retrieval systems like Elasticsearch, on which the DIG backend is based, make this easier on the engineering front by accepting multiple weighted queries as input as a *forest* of queries, and producing a final set of ranked results through combining and re-ranking. This final set of results is then displayed to the user. By leveraging advances in IR, including advanced indexing methods, results can be retrieved quickly.

Figure 5. An illustration of query reformulation



One aspect of an illicit domain DSS that should never be underestimated is the design of the Graphical User Interface (GUI) that the non-technical user uses to access the system. The backend of the system, including the actual query posed against Elasticsearch, should be insulated from such users. However, the user should still be given control both over KGC and over the search itself. Considerable research and user testing was conducted on systems like DIG to ensure that users were equipped to handle and remember system functionalities. In the case of KGC, users were shown how to define their investigative schema and declare meta-attributes like the importance of fields, whether the field should be visible to search against, the data type (e.g., numeric vs. string) of the field etc. Users were also able to handle expressive search facilities, including when to declare a specification as optional. A visualization of the search form was earlier shown in Figure 2.

FUTURE RESEARCH DIRECTIONS

Despite enormous progress under the DARPA Memex program and several others before it, domain-specific search (DSS) continues to be an important problem that is amenable to interesting exploration. One action item that the community should adopt is to assess the adoption of the technology described herein to illicit domains other than human trafficking (HT). Several promising domains for which DSS feasibility and pilot implementations have already been explored (but not significantly expanded, as in the case of HT) are enumerated below:

- **Counterfeit Electronics Sales:** Despite what the name suggests, investigators in the counterfeit electronics domain are interested, not in consumer electronics, but in microchips and field-programmable gate arrays (FPGAs) that form the computational backbones of more complex devices. The FPGAs may resemble an FPGA from a genuine contractor, but are fakes, and may have malicious modifications at the hardware level. Certain countries, companies and devices are more relevant to this kind of activity than others. Note that there is an obvious national security component to these investigations, and just like with the other described domains, domain expertise plays a crucial role both in setting up the domain, and in the knowledge discovery itself. The ability of a DSS to be set up on private infrastructure or premises is especially important in matters of national security, though generally, the requirement emerges an important one in almost every domain of an investigative nature.
- **Mail Shipment Fraud:** Illicit shipments via USPS happen in the physical world but *communications* about the illicit shipment, particularly tracking numbers, happen *digitally* in specific forums and typologies that investigators in this domain understand well. DSS can help investigators find and crawl information across multiple sources (domain discovery) and then aggregate and compartmentalize this information according to specific investigative needs.
- **Securities Fraud:** Securities, particularly *penny stock*, fraud is a complex and unusual domain because much of the activity that accompanies fraudulent behavior, including hype and promotional activity, is legally permitted. Many of the actual actors involved may not be physically present in the US, but for regulatory reasons, ‘shell’ companies fronting such activity for promotional and legal purposes, have to be registered in the US to trade stocks legitimately in over-the-counter exchanges. In addition to the longer-term goal of investigating, and gathering information on, such shell companies and the people involved in them, investigators are also interested in taking preventive activity. This can happen when a penny stock company is caught actively engaging in

factually (i.e. provable) fraudulent hype (for example, a false claim that a contract was just signed with a well-known customer firm), in which case trading can be halted or even shut down. DSS can support these investigate and preventive goals by allowing users to aggregate information about suspicious penny stocks crawled over the Web, zero in on burgeoning promotional activity and compile dossiers to discern patterns between multiple stocks.

- **Illegal Firearms Sales:** In the US, firearms sales are regulated in that transactions cannot be conducted over arbitrary channels like the Internet. Investigators in this domain are interested in pinpointing activity that, either directly or indirectly, provides evidence for illicit online sales of firearms that leave some digital trace. The domain is similar to the securities fraud domain (and dissimilar to the counterfeit electronics sales domain) for the important reason that investigators tend to limit their focus to *domestic* activities.

CONCLUSION

This article explored the problem of domain-specific search (DSS) for illicit domains that have exploited the Web to gain increased market share. The human trafficking domain, where this problem has been most explored, was used as a clarifying example both in terms of the challenges and recommendations involved. Although much progress has been made, and the solutions described in this article have been adopted into real systems that have been used by law enforcement for convicting traffickers, much work still remains to be done. In particular, the findings need to be extended and tested on other illicit domains. The scope of the DSS can also be significantly expanded. One avenue for future exploration is to enable natural language question answering and conversational interfaces so that investigators can access the system even more intuitively. Finally, as existing AI technology for information extraction and knowledge graph construction continue to improve, an engineering challenge is to ‘roll out’ updates to different modules in a way that does not have unexpected negative consequences on the system’s behavior. This is a general challenge with composing and using multiple AI technologies, and DSS is no different.

REFERENCES

- Aggarwal, C. C., Al-Garawi, F., & Yu, P. S. (2001, April). Intelligent crawling on the World Wide Web with arbitrary predicates. In *Proceedings of the 10th international conference on World Wide Web* (pp. 96-105). ACM. 10.1145/371920.371955
- Alvari, H., Shakarian, P., & Snyder, J. K. (2016, September). A non-parametric learning approach to identify online human trafficking. In *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on* (pp. 133-138). IEEE. 10.1109/ISI.2016.7745456
- Alvari, H., Shakarian, P., & Snyder, J. K. (2017). Semi-supervised learning for detecting human trafficking. *Security Informatics*, 6(1), 1. doi:10.1186/13388-017-0029-8
- Andolina, S., Klouche, K., Ruotsalo, T., Floréen, P., & Jacucci, G. (2018). Querytogether: Enabling entity-centric exploration in multi-device collaborative search. *Information Processing & Management*, 54(6), 1182–1202. doi:10.1016/j.ipm.2018.04.005

- Angeli, G., Premkumar, M. J. J., & Manning, C. D. (2015). Leveraging linguistic structure for open domain information extraction. In *Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing* (Vol. 1, pp. 344-354). 10.3115/v1/P15-1034
- Barrio, P., & Gravano, L. (2017). Sampling strategies for information extraction over the deep web. *Information Processing & Management*, 53(2), 309–331. doi:10.1016/j.ipm.2016.11.006
- Bhutani, N., Jagadish, H. V., & Radev, D. (2016). Nested propositions in open information extraction. In *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing* (pp. 55-64). 10.18653/v1/D16-1006
- Bollacker, K., Evans, C., Paritosh, P., Sturge, T., & Taylor, J. (2008, June). Freebase: a collaboratively created graph database for structuring human knowledge. In *Proceedings of the 2008 ACM SIGMOD international conference on Management of data* (pp. 1247-1250). ACM. 10.1145/1376616.1376746
- Brambilla, M., Ceri, S., & Halevy, A. (2013). Special issue on structured and crowd-sourced data on the Web. *The VLDB Journal*, 22(5), 587–588. doi:10.1007/00778-013-0327-9
- Burbano, D., & Hernandez-Alvarez, M. (2017, October). Identifying human trafficking patterns online. In *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6). IEEE.
- Chang, C. H., Kayed, M., Girgis, M. R., & Shaalan, K. F. (2006). A survey of web information extraction systems. *IEEE Transactions on Knowledge and Data Engineering*, 18(10), 1411–1428. doi:10.1109/TKDE.2006.152
- Chen, H. (2011). *Dark web: Exploring and data mining the dark side of the web* (Vol. 30). Springer Science & Business Media.
- Dalvi, N., Kumar, R., Pang, B., Ramakrishnan, R., Tomkins, A., Bohannon, P., ... Merugu, S. (2009, June). A web of concepts. In *Proceedings of the twenty-eighth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (pp. 1-12). ACM.
- Doan, A., Halevy, A., & Ives, Z. (2012). *Principles of data integration*. Elsevier.
- Doddington, G. R., Mitchell, A., Przybocki, M. A., Ramshaw, L. A., Strassel, S., & Weischedel, R. M. (2004, May). The Automatic Content Extraction (ACE) Program-Tasks, Data, and Evaluation. In *LREC* (Vol. 2, p. 1). Academic Press.
- Dong, X. L., & Srivastava, D. (2013, April). Big data integration. In *Data Engineering (ICDE), 2013 IEEE 29th International Conference on* (pp. 1245-1248). IEEE. 10.1109/ICDE.2013.6544914
- El-Masri, R., & Wiederhold, G. (1979, May). Data model integration using the structural model. In *Proceedings of the 1979 ACM SIGMOD international conference on Management of data* (pp. 191-202). ACM. 10.1145/582095.582127
- Elmagarmid, A. K., Ipeirotis, P. G., & Verykios, V. S. (2007). Duplicate record detection: A survey. *IEEE Transactions on Knowledge and Data Engineering*, 19(1), 1–16. doi:10.1109/TKDE.2007.250581
- Ernst, P., Siu, A., Milchevski, D., Hoffart, J., & Weikum, G. (2016). Deeplife: An entity-aware search, analytics and exploration platform for health and life sciences. *Proceedings of ACL-2016 System Demonstrations*, 19-24. 10.18653/v1/P16-4004

- Etzioni, O., Banko, M., Soderland, S., & Weld, D. S. (2008). Open information extraction from the web. *Communications of the ACM*, 51(12), 68–74. doi:10.1145/1409360.1409378
- Frank, J. R., Kleiman-Weiner, M., Roberts, D. A., Niu, F., Zhang, C., Ré, C., & Soboroff, I. (2012). *Building an entity-centric stream filtering test collection for TREC 2012*. Massachusetts Inst of Tech.
- Freitas, A., Curry, E., Oliveira, J. G., & O’Riain, S. (2012). Querying heterogeneous datasets on the linked data web: Challenges, approaches, and trends. *IEEE Internet Computing*, 16(1), 24–33. doi:10.1109/MIC.2011.141
- Gabrilovich, E., & Markovitch, S. (2007, January). Computing semantic relatedness using wikipedia-based explicit semantic analysis. *IJCAI (United States)*, 7, 1606–1611.
- Gamallo, P., & Garcia, M. (2015, September). Multilingual open information extraction. In *Portuguese Conference on Artificial Intelligence* (pp. 711-722). Springer.
- Getoor, L., & Machanavajjhala, A. (2012). Entity resolution: Theory, practice & open challenges. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 5(12), 2018–2019. doi:10.14778/2367502.2367564
- Gomez-Cabrero, D., Abugessaisa, I., Maier, D., Teschendorff, A., Merkschlager, M., Gisel, A., ... Tegnér, J. (2014). *Data integration in the era of omics: current and future challenges*. Academic Press.
- Gupta, N., Halevy, A. Y., Harb, B., Lam, H., Lee, H., Madhavan, J., . . . Yu, C. (2013, April). Recent progress towards an ecosystem of structured data on the Web. In *2013 IEEE 29th International Conference on Data Engineering (ICDE)* (pp. 5-8). IEEE. 10.1109/ICDE.2013.6544808
- Hultgren, M., Jennex, M. E., Persano, J., & Ornatowski, C. (2016, January). Using knowledge management to assist in identifying human sex trafficking. In *System Sciences (HICSS), 2016 49th Hawaii International Conference on* (pp. 4344-4353). IEEE. 10.1109/HICSS.2016.539
- Kejriwal, M., Ding, J., Shao, R., Kumar, A., & Szekely, P. (2017). *FlagIt: A system for minimally supervised human trafficking indicator mining*. arXiv preprint arXiv:1712.03086
- Kejriwal, M., & Szekely, P. (2017a, April). Information extraction in illicit web domains. In *Proceedings of the 26th International Conference on World Wide Web* (pp. 997-1006). International World Wide Web Conferences Steering Committee. 10.1145/3038912.3052642
- Kejriwal, M., & Szekely, P. (2017b). Knowledge graphs for social good: an entity-centric search engine for the human trafficking domain. *IEEE Transactions on Big Data*, (1), 1-1.
- Kejriwal, M., & Szekely, P. (2017c, October). An Investigative Search Engine for the Human Trafficking Domain. In *International Semantic Web Conference* (pp. 247-262). Springer. 10.1007/978-3-319-68204-4_25
- Kejriwal, M., Szekely, P., & Knoblock, C. (2018). Investigative Knowledge Discovery for Combating Illicit Activities. *IEEE Intelligent Systems*, 33(1), 53–63. doi:10.1109/MIS.2018.111144556
- Krishnamurthy, Y., Pham, K., Santos, A., & Freire, J. (2016). Interactive exploration for domain discovery on the web. *Proc. of KDD IDEA*.

Kushmerick, N., Weld, D. S., & Doorenbos, R. (1997). *Wrapper induction for information extraction*. Academic Press.

Leng, J., & Jiang, P. (2016). A deep learning approach for relationship extraction from interaction context in social manufacturing paradigm. *Knowledge-Based Systems*, 100, 188–199. doi:10.1016/j.knosys.2016.03.008

Lenzerini, M. (2002, June). Data integration: A theoretical perspective. In *Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (pp. 233-246). ACM. 10.1145/543613.543644

Lerman, K., Minton, S. N., & Knoblock, C. A. (2003). Wrapper maintenance: A machine learning approach. *Journal of Artificial Intelligence Research*, 18, 149–181. doi:10.1613/jair.1145

Loshin, D. (2013). *Big data analytics: from strategic planning to enterprise integration with tools, techniques, NoSQL, and graph*. Elsevier.

Martinez-Rodriguez, J. L., Hogan, A., & Lopez-Arevalo, I. (2018). Information extraction meets the Semantic Web: A survey. *Semantic Web*, (Preprint), 1-81.

McKeown, S., Buivys, M., & Azzopardi, L. (2016, July). InfoScout: An Interactive, Entity Centric, Person Search Tool. In *Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval* (pp. 1113-1116). ACM. 10.1145/2911451.2911468

Miller, G. A. (1995). WordNet: A lexical database for English. *Communications of the ACM*, 38(11), 39–41. doi:10.1145/219717.219748

Muslea, I., Minton, S., & Knoblock, C. (1998, July). Stalker: Learning extraction rules for semistructured, web-based information sources. In *Proceedings of AAAI-98 Workshop on AI and Information Integration* (pp. 74-81). AAAI Press.

Nam, D., & Kejriwal, M. (2018). How Do Organizations Publish Semantic Markup? Three Case Studies Using Public Schema.org Crawls. *Computer*, 51(6), 42–51. doi:10.1109/MC.2018.2701635

Niu, F., Zhang, C., Ré, C., & Shavlik, J. W. (2012). DeepDive: Web-scale Knowledge-base Construction using Statistical Learning and Inference. *VLDS*, 12, 25–28.

Pantel, P., Gamon, M., Kannan, A., Fuxman, A., & Lin, T. (2017). *U.S. Patent No. 9,767,201*. Washington, DC: U.S. Patent and Trademark Office.

Paulheim, H. (2017). Knowledge graph refinement: A survey of approaches and evaluation methods. *Semantic Web*, 8(3), 489–508. doi:10.3233/SW-160218

Pennington, J., Socher, R., & Manning, C. (2014). Glove: Global vectors for word representation. In *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)* (pp. 1532-1543). 10.3115/v1/D14-1162

Qiu, J. X., Yoon, H. J., Fearn, P. A., & Tourassi, G. D. (2018). Deep learning for automated extraction of primary sites from cancer pathology reports. *IEEE Journal of Biomedical and Health Informatics*, 22(1), 244–251. doi:10.1109/JBHI.2017.2700722 PMID:28475069

- Rabbany, R., Bayani, D., & Dubrawski, A. (2018, July). Active search of connections for case building and combating human trafficking. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 2120-2129). ACM. 10.1145/3219819.3220103
- Roberts, D. A., Kleiman-Weiner, M., Frank, J. R., Olson, B. A., Maze, D. Z., Gallant, A. R., . . . DuBois, T. M. (2016). *U.S. Patent No. 9,275,132*. Washington, DC: U.S. Patent and Trademark Office.
- Saleiro, P., Teixeira, J., Soares, C., & Oliveira, E. (2016, March). Timemachine: Entity-centric search and visualization of news archives. In *European Conference on Information Retrieval* (pp. 845-848). Springer. 10.1007/978-3-319-30671-1_78
- Singhal, A. (2012). Introducing the knowledge graph: things, not strings. *Official Google Blog*, 5.
- Szekely, P., Knoblock, C. A., Slepicka, J., Philpot, A., Singh, A., Yin, C., ... Stallard, D. (2015, October). Building and using a knowledge graph to combat human trafficking. In *International Semantic Web Conference* (pp. 205-221). Springer. 10.1007/978-3-319-25010-6_12
- Tonon, A., Demartini, G., & Cudré-Mauroux, P. (2012, August). Combining inverted indices and structured search for ad-hoc object retrieval. In *Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval* (pp. 125-134). ACM. 10.1145/2348283.2348304
- Whitney, J., Jennex, M., Elkins, A., & Frost, E. (2018). *Don't Want to Get Caught? Don't Say It: The Use of EMOJIS in Online Human Sex Trafficking Ads*. Academic Press.
- Yan, X., Song, D., & Li, X. (2006, November). Concept-based document readability in domain specific information retrieval. In *Proceedings of the 15th ACM international conference on Information and knowledge management* (pp. 540-549). ACM. 10.1145/1183614.1183692

ADDITIONAL READING

- Doan, A., Ramakrishnan, R., & Vaithyanathan, S. (2006, June). Managing information extraction: state of the art and research directions. In *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*(pp. 799-800). ACM. 10.1145/1142473.1142595
- Greiman, V., & Bain, C. (2013, January). The emergence of cyber activity as a gateway to human trafficking. In *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW* (p. 90).
- Hogan, A., Harth, A., Umrich, J., & Decker, S. (2007, May). Towards a scalable search and query engine for the web. In *Proceedings of the 16th international conference on World Wide Web* (pp. 1301-1302). ACM. 10.1145/1242572.1242819
- Kapoor, R., Kejriwal, M., & Szekely, P. (2017, May). Using contexts and constraints for improved geo-tagging of human trafficking webpages. In *Proceedings of the Fourth International ACM Workshop on Managing and Mining Enriched Geo-Spatial Data* (p. 3). ACM. 10.1145/3080546.3080547
- Lin, T., Pantel, P., Gamon, M., Kannan, A., & Fuxman, A. (2012, April). Active objects: Actions for entity-centric search. In *Proceedings of the 21st international conference on World Wide Web* (pp. 589-598). ACM.

Marchionini, G. (2006). Exploratory search: From finding to understanding. *Communications of the ACM*, 49(4), 41–46. doi:10.1145/1121949.1121979

Pantel, P., Crestan, E., Borkovsky, A., Popescu, A. M., & Vyas, V. (2009, August). Web-scale distributional similarity and entity set expansion. In *Proceedings of the 2009 Conference on Empirical Methods in Natural Language Processing: Volume 2-Volume 2* (pp. 938-947). Association for Computational Linguistics. 10.3115/1699571.1699635

Savona, E. U., & Stefanizzi, S. (Eds.). (2007). *Measuring human trafficking: Complexities and pitfalls*. Springer Science & Business Media. doi:10.1007/0-387-68044-6

KEY TERMS AND DEFINITIONS

Domain-Specific Search (DSS): The problem of building a (rudimentary or advanced) search engine over a domain-specific corpus. Domains of special interest in this article were illicit domains such as human trafficking, over which building such an engine is an especially challenging problem.

Entity Resolution: Entity resolution (ER) is the problem of algorithmically determining when two entities in a KG refer to the same underlying entity. For example, the same entity ‘Barack Obama’ may have been independently extracted from two webpages under names such as ‘President Obama’ and ‘Obama’.

Information Extraction (IE): Information extraction (IE) is an algorithmic technique that generally accepts as input either text or raw HTML as input, and outputs a set of ontologically typed instances. For illicit domains, the investigative schema serves as the ontology. Supervised machine learning and deep learning IE methods have emerged as state-of-the-art in recent times.

Investigative Schema: An investigative schema is an ontology expressing an investigative domain of interest, usually involving an illicit activity like sex advertising. The investigative schema is usually simple and shallow, hence the term ‘schema’ and not ‘ontology’.

Knowledge Graph (KG): A knowledge graph (KG) is a directed, labeled multi-relational graph that is used to model and represent semi-structured data to make it more amenable to machine reasoning (‘knowledge’).

Ontology: An ontology may be practically defined as a controlled set of terms and constraints for expressing the domain of interest. An ontology can range from a simple set of terms (e.g., {PERSON, LOCATION, ORGANIZATION}) to a taxonomy (with concepts and sub-concepts e.g., ACTOR and ENTREPRENEUR would be sub-concepts of PERSON) to a general graph with equational constraints e.g., that the domain and range of the relation *starred-in* is ACTOR and MOVIE respectively. Any KG that is ontologized thus should obey such constraints at the instance level.

Query Reformulation: Query reformulation refers to a set of techniques wherein a query (in some domain-specific language like SPARQL or SQL) that is originally posed against a DSS engine is reformulated into a set of queries (in the same or different language) to increase query retrieval performance. Query reformulation is a useful technique both when the underlying KG is noisy and when the original query does not fully express (or over-conditions) user intent.

ENDNOTES

- ¹ This terminology is non-traditional and was set by DARPA and NIST over the course of the DARPA Memex evaluations.
- ² A general description of the Memex program can be accessed at <https://www.darpa.mil/program/memex>. Domain-specific search technology developed under Memex can be used for constructing and using DSS engines not just for illicit domains, but also non-illicit domains. Many of the tools have been released as open source under permissive licenses.

Identifying Victims of Human Sex Trafficking in Online Ads

Jessica Whitney

San Diego State University, USA

Marisa Hultgren

 <https://orcid.org/0000-0002-3528-9831>

San Diego State University, USA

Murray Eugene Jennex

 <https://orcid.org/0000-0003-4332-1886>

San Diego State University, USA

Aaron Elkins

San Diego State University, USA

Eric Frost

San Diego State University, USA

INTRODUCTION

Trafficking humans for sexual exploitation is a fast-growing criminal enterprise even though international law and the laws of 158 countries criminalize sex trafficking (Equality Now, 2017). The Equality Now (2017) *Sex Trafficking Fact Sheet* lists these statistics:

- Sex trafficking is a lucrative industry that makes an estimated US\$99 billion a year.
- About two million children are exploited every year in the global commercial sex trade.
- Women and girls make up 96 percent of victims of trafficking for sexual exploitation.

Further, human trafficking is not just a third or developing world problem. The National Human Trafficking Resource Center hotline lists 5784 human sex trafficking cases reported in the United States during 2016 (NHTRC, 2018a). Additionally, the National Human Trafficking Resource Center has reported that California had 1050 of these cases (NHTRC, 2018). (Note that this chapter and research uses a sample set from California, United States and so statistics, policies, and laws used in this chapter are focused on this region)

The U.S. Government defines human trafficking as inducing others to perform a commercial sex act by force, fraud, or coercion; as inducing a person under 18 years of age for such an act; and/or as recruiting, harboring, transporting, providing, obtaining a person for labor or services through the use of force, fraud, or coercion in order to subject them to involuntary servitude, peonage, debt bondage, or slavery (National Institute of Justice, 2012). However, the Department of Homeland Security (DHS) has more recently shortened the definition of human trafficking to a contemporary form of slavery that

DOI: 10.4018/978-1-5225-9715-5.ch034

involves the illegal trade of people for exploitation or commercial gain (Department of Homeland Security, 2014). Further clarifying this definition, California's Department of Justice (DOJ) has stated that human trafficking is a contemporary form of slavery that involves controlling a person through force, fraud, or coercion to exploit the victim for forced labor, sexual exploitation, or both (Harris, 2012). While slightly different, all three definitions are similar in context. However, for this paper, we use California's DOJ's definition but note that two classes of human sex trafficking exist: those for victims under 18 (minors) and those for 18 or over.

In this paper, we focus on the sex trafficking aspect of human trafficking and propose an information systems approach to identify sex trafficking victims based on analyzing online (Internet) ads. We focus on online ads because social media and the interactive Web have enabled traffickers to lure victims and sell them at a faster rate and in greater safety than ever before. However, these same tools have also created new avenues for prosecution and criminal investigations for law enforcement as officials now have access to a vast amount of information about the sex industry. We use system development methodology from action research (Nunamaker, Chen, & Purdin, 1990; Burstein & Gregor, 1999) with a knowledge management strategy approach of identifying actionable intelligence (i.e., identifying victims of human sex trafficking) by applying a set of strong filters based on an ontology of keywords that codifies attributes of human sex trafficking victims to assess an unstructured dataset consisting of the text from online ads scraped from the women looking for men section of backpage.com.

Specifically, we address the following research question:

RQ: Can one use online data to identify victims of human sex trafficking?

To answer this question, we created a prototype to explore text-based indicators of human trafficking in online classified ads (see section 4.1 for a list of these terms). In particular, we created the prototype to:

- Create an ontology/keyword list of terms and/or attributes that may indicate human trafficking
- Create a process for extracting an unstructured text dataset from online advertising, and
- Use the keyword ontology to construct strong filters that can be applied to the unstructured dataset to determine ads that create actionable intelligence on identifying victims of human sex trafficking.

Additionally, during the study of keywords in online ads we discovered that emojis were being used in lieu of keywords leading to the addition of the following purpose for the final prototype (see section 5.2.2 for the emojis identified as being used in human sex trafficking):

- Add emojis to the keyword ontology and use them to construct strong filters that can be applied to the unstructured dataset to determine ads that create actionable intelligence on identifying victims of human sex trafficking.

The prototype we created utilized: Strong filters that combined knowledge/experience-driven ontologies of keywords and emojis that modeled human sex trafficking victims

- A process for updating the ontology
- A process for extracting an unstructured dataset of online ads, and
- A process for analyzing the unstructured dataset using evaluation criteria for determining what ads are actionable

Technologies in the prototype included ontologies, machine learning, text mining, and Web scrapers.

KNOWLEDGE MANAGEMENT, TECHNOLOGIES, AND TRAFFICKING INDICATORS

3

Knowledge Management

We used a knowledge management, KM, approach to develop and apply ontologies (defined later) to create strong filters to help identify potential victims of human sex trafficking in online advertising. In this section, we review the literature and theoretical base for using knowledge management to help develop a system implementation to assist in searching for human sex trafficking victims.

Jennex (2005) defines KM as the practice of selectively applying knowledge from previous decision making experiences to current and future decision making activities to improve an organization's effectiveness. Jennex (2017) incorporates big data and the Internet of things (IoT) (see Figure 1 below) into Jennex and Bartczak's (2013) modified knowledge pyramid and uses the final revised pyramid to define the purpose of KM as identifying, generating, capturing, and using actionable intelligence. Actionable intelligence is that knowledge that can be directly and immediately applied to make a decision. KM processes filter IoT, big data, data, information, and knowledge to generate specific, actionable intelligence that the organization can share with specific, limited users. Additionally, Jennex (2017) places filters on social networks to limit access and to separate and capture that which the organization needs from that which it does not. In this vein, "filters" is a fairly new term for KM, and we view KM filters as the implementation of KM strategy. While KM requires all the components in the figure and we use them all in this research, we consider KM strategy and KM content the most important in designing and implementing the prototype that we present in this paper. KM strategy determined needed actionable intelligence, guided us in determining what data and information to collect, and finally guided us in designing and constructing the filters.

Filters were designed using ontologies. Ontologies codify knowledge by providing a simplified and explicit specification of a phenomenon that one desires to represent (Gruber, 1995; Noy and McGuinness, 2001; Staab, et al., 2001). Ontologies are useful because they explicate components that define a phenomenon and, thus, can help in systematically understanding or modeling that phenomenon (Holsapple & Joshi, 2004). Keywords/terms are specific examples from an ontology with a complete set of keywords/terms that define an ontology. Alavi and Leidner (2001, p. 114) define a KMS as "IT (Information Technology) based systems developed to support and enhance the organizational processes of knowledge creation, storage/retrieval, transfer, and application". Many researchers include ontologies in the KMS as tools for organizing and retrieving knowledge (Aldea et al., 2003; Almeida & Barbosa, 2009; Holsapple & Joshi, 2004; Jurisica, Mylopoulos, & Yu, 1999; Varma, 2007; Wu & Yang, 2005).

We created ontologies by identifying keywords from the experience literature that describes the phenomenon of human sex trafficking. We then used our first ontology in a KMS that applied the ontology to a set of unstructured ad data to create actionable intelligence that we could use to identify potential victims of human sex trafficking in online advertising. Subsequently, we created a new ontology based on more current literature and a second dataset and then used machine learning tools to enhance this ontology based on patterns in the ad dataset and applied the enhanced ontology to identify potential victims of human sex trafficking in the second dataset. In the future, we plan to use machine learning tools to automatically generate an ontology from a new dataset.

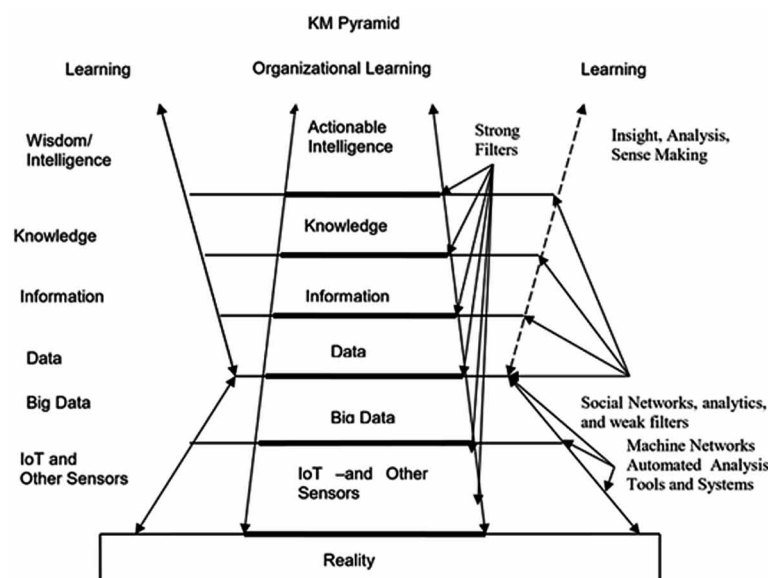
Technologies for Combatting Trafficking

Amin (2010) discusses the potential benefits of using machine learning as a tool to combat human trafficking. These benefits include; detecting features and unusual patterns indicative of potential cases of human trafficking, identifying rules that can assist in predicting trafficking activity and profiling victims and criminals, and help in automating pattern identification and search process for potential instances of trafficking online. One application of machine learning techniques for combatting online sex trafficking involved the use of a sample of backpage.com ads from March 2016 to train a learning classifier. The ads collected from backpage.com were first filtered using known indicators of online sex trafficking and feature engineering. The six categories used for creating the feature set included; ad language pattern, words and phrases of interest, countries of interest, ad of multiple victims, weight of victim, and whether the ad reference an external website or spa massage therapy. Following this unsupervised filtering, a small portion of the remaining ads were then labeled by human experts as to whether they were instances of human sex trafficking. A semi supervised learning algorithm was then used to label the remaining ads and the classifications were then reviewed by experts in online sex trafficking to evaluate accuracy. Radial basis function (92.41% True Positive Rate) and K-nearest neighbor (90.42% True Positive Rate) kernels were used to assign classifications and both learning models were able to predict online instances of sex trafficking with high accuracy (Alvari, Shakarian, and Snyder, 2016). This study indicates the high potential of using machine learning techniques to identify ads that are potentially human trafficking related. Additionally, the use of semi-supervised methods makes the modeling technique more realistic for real world application because obtaining large enough samples of labeled data for a purely supervised learning algorithm is not very plausible.

Dubrawski, et al. (2015) trained multiple random forest models using three differed information extraction approaches, term-frequency analysis using law enforcement provided keywords, regular expressions, and natural language processing. Of these three, the natural language processing feature set

Figure 1. The final revised knowledge pyramid

Source: Jennex, 2017



had the highest accuracy in predicting actual instances of human sex trafficking, lowest false positive rate, followed by the keyword feature extraction method. The natural language processing feature set was obtained by compiling a bag of words from online escort ads and then using principle component analysis for dimensionality reduction (Dubraski, et al., 2015).

Research on the use of machine learning techniques to combat child sex trafficking has also involved the architectural design and prototyping of Traffic Bot and WAT – Web Archival Tool, its successor. Traffic Bot crawls websites known for ad postings for escort and massages services to collect data and then provides an interface to drill down the collected ad data based on phone numbers as a tool to identify potential cases of sex trafficking. Wang, et al. (2014) in designing the Traffic Bot framework examined how classified escort ads disguise phone numbers with the use of unusual punctuation and spelling and character or word substitution. They identified a regular expression method to be effective in detecting and decoding these phone numbers and used this technique as their filtering method. They were able to detect ads where the same phone number was listed for different women or multi-person services, two indicators of potential trafficking. They also note that by using the interface to drill down by phone number and identify instances where the area code differed from the location of the ad posting, one may be able to identify the location of a home base (Wang, et al., 2014). WAT – Web Archival Tool was geared specifically at identifying underage victims of sex trafficking (Hovy, et al., 2014). Hovy et al. (2014) clustered data collected via a daily web crawler of websites advertising escort services based on relationships between the postings themselves or poster of the ad. The system facilitated dynamic cluster movement as new data was added and provide three interfaces with which to analyze the resulting clusters (Hovy, et al., 2014).

These technologies are used to enhance KM and fit into KM/KMS as shown in Figure 1. Figure 1 shows that these technologies are used to construct filters that are used to convert data to information, knowledge, and actionable intelligence. Additionally, these filters assist users in generating sense making from the data, information, knowledge and actionable intelligence.

Indicators of Sex Trafficking in Ads

We reviewed the literature for research that focused on identifying victims of sex trafficking through indicators found in ads. We reviewed these indicators for those that we could operationalize through a set of key words/ontology. The below list and literature reflects those indicators that met this requirement.

Movement Between Cities

Ads that evidence frequent movement, or transience, may signal that a sex worker is a victim of trafficking. Pimps often move victims around from city to city in order to avoid law enforcement and to maintain control by keeping victims from building a social support system or becoming too familiar with a particular area (Dank et al., 2014). This movement also keeps victims disoriented and ignorant of where to seek help (Harris, 2012). However, pimps tend to move victims in groups or stables. Ultimately, this steady movement leaves women and girls consistently vulnerable to those who control them. Indeed, a study on trafficking in Silicon Valley found that traffickers often move sex workers around the Bay Area (Juniper Networks, 2014). The frequent movement between cities also has a marketing side. It serves to maintain a “fresh” product line for clients (Harris, 2012). In this way, traffickers constantly circulate “new product” to entice consumers (Ibanez & Suthers, 2014). They often move international women from the East to the West Coast, South to Northeast, and from urban to rural and vice versa. American

women are trafficked across city and state borders and internationally (Raymond, Hughes, & Gomez, 2001). Additionally, traffickers may post ads in other cities to gauge the market in that area based on the amount of hits they get (Dank et al., 2014). By analyzing phone numbers posted in ads, researchers can identify area code networks in online escort service ads that can further identify patterns of victim movement in a geographical area (Ibanez and Suthers, 2014).

Ethnicity and National Origin

Ibanez and Suthers (2014) reference the denotation of ethnicity as a possible sign of trafficking. One needs to use this indicator in context of the dataset one analyzes before including it as an indicator to ensure that the dataset uses a variety of ethnicities/national origins because an estimated 72 percent of sex trafficking victims in California are American citizens. Thus, being “American” is not effective as an ethnicity or national origin term for identifying a potential trafficking victim.

Restricted Movement

Law enforcement officials believe that pimps consider it safer to conduct activities online and use incalls only (Dank et al., 2014). Previous studies have used restricted movement seen through terms such as “incalls only” as a possible indicator of sex trafficking (Ibanez & Suthers, 2014). To control their victims, perpetrators often deny them their freedom of movement and keep them isolated.

Unconventional Sex

One ad that researchers found to advertise a victim of sex trafficking included the term “open minded” (Operation Broken Silence, 2012), which may be a code word that signifies that customers can perform unconventional and sadistic types of sex. As such, an ad with such a phrase may increase the likelihood that the sex worker it advertises is a victim of trafficking (Yen, 2008).

Minors Trafficked Online

Sellers solicit buyers who are interested in purchasing young girls (often minors) using certain keywords that can indicate a sex trafficking victim. Ads for underage victims sometimes use words such as: fresh, fresh meat, young, virgin, prime, coochie (shaved), non-pro, new, new in town, barely legal/18, college student/girl, lovely, daddy’s little girl, sweet, 1986 Firebird, new in the life, liked girls, youthful, and fantasy (Bouche, 2015; Boyd, Casteel, Thakor, & Johnson, 2011; Major, 2012).

Phone Numbers and Area Codes

Classified ads often include phone numbers. Customers and sellers sometimes use them to look up reviews on a particular girl and to see if the girl has alternate names (Ibanez & Suthers, 2014). Traffickers and victims often use multiple (both contract and disposable) phones in sex trafficking operations. Latonero et al. (2012) looked at the distribution of phone numbers using a simple Google search and found the phone number of one suspected victim on seven other escort service websites for multiple cities. Additionally, they found the same phone number on MyRedBook with a different name but similar photographs. This widespread advertisement across the Internet and geographic regions indicates

more than just alone prostitute out to make extra money. It could even indicate a sex trafficking ring. Information from area codes strongly indicates the movement of victims and traffickers. The area code network offers both a source and destination. One can generate maps to determine suspected routes that sex traffickers use to transport victims from one location to another.

METHODOLOGY

System Development Method

We used the systems development research methodology from action research that Nunnemaker et al. (1990) and Burstein and Gregor (1999) describe. We chose this methodology in order to produce a system that combines technology with social understanding for detecting ads that offer the services of victims of human sex trafficking. Systems development research methodology is a multimethodological conceptual approach that incorporates theory building, experimentation, and observation into systems building. System building is a form of applied research that focuses on solving a specific problem. Further, the system development method theory uses observation, and experimentation (or prototyping) methodologies to create the system. The system development method has five basic steps:

1. Identify and/or generate theory applicable to solving an information system (IS) problem. The system development method does not need to create this theory, but one can instead use it to design and build a prototype system to test or implement the theory in solving the IS problem (see second to fifth steps).
2. Create the concept for the proposed system.
3. Design and develop the proposed system.
4. Apply and use the proposed system.
5. Evaluate the success of the proposed system in meeting one's research question or goals.

In this study, we accomplished the first two steps using the literature review. Thus, in the first step, we identified and used the literature related to indicators of human sex trafficking in ads to create an initial ontology. In the second step, we identified and applied the KM concept of using a set of strong filters based on the ontology in a KMS designed to assess a dataset of ads. In the third step, we created the prototype by actually generating the ontology/keywords and identifying processes for obtaining a dataset, verifying the ontology/keywords against the dataset, and applying the ontology/keywords in order to analyze that dataset. In the fourth step, we applied the prototype that utilized the ontology/keywords and the processes that we created in the third step to assess a dataset for identifying victims of human sex trafficking. In step five, we evaluated the results from the fourth step and the proposed system to determine if the proposed system could accurately identify victims of human sex trafficking.

Literature Review Method

We identified the appropriate literature using the following search terms in various combinations: “sex trafficking”, “human trafficking”, “United States”, “America”, “California”, “online”, “Internet”, “social media”, “backpage”, “craigslist”, “classifieds”, “ontology”, “emojis”, and “technology”. We began the literature review using Google Scholar to find papers that have received a high number of citations and

to establish a baseline of pertinent literature. We conducted further searches using databases such as Ebscohost-Academic Search Premier, Scribd, and JSTOR. We used papers' references that particularly related to this study to find other similarly related papers. Finally, we searched the *Journal of Human Trafficking*'s archives.

Interview Method

As follow up to the literature review, we conducted unstructured interviews with law enforcement and individuals involved in efforts to combat online human sex trafficking and with academic researchers with expertise in the area of technology and human trafficking. Specifically, we interviewed a San Diego County's Sheriff's Department sergeant who was a member of their joint-agency human trafficking task force and two University of Southern California faculty members involved in Department of Justice and Humanity United-funded research projects focused on creating a better understanding of the role of technology in human trafficking activities and the use of data analytics to combat sex trafficking. We selected these interview subjects based on their availability, and a single interviewer conducted them in order to avoid bias. The interviews consisted of two-open ended questions:

- Explain your main areas of research/methods for targeting and identifying online trafficking activities?
- How have you applied your knowledge of the language that traffickers use (ontologies) to efforts to combat or identify online sex trafficking activities?

Based on their responses, we asked the respondents to expand on certain areas that we deemed required a more detailed explanation. We intended these interviews to confirm the practical application of theory identified through the literature review and identify any additional knowledge areas the theory did not address. We identified several highlights. First, the human trafficking task force believes that an ad that features a sex worker as 25 years old or younger is most likely a minor. Second, the interviewees noted that one needs to consider the social implications in using technology to identify online human trafficking. Finally, they discussed the difficulty in distinguishing between trafficking and non-trafficking ads and the best approach to address this issue.

SYSTEM PROTOTYPE DEVELOPMENT

KM focuses on producing actionable intelligence. In this research, the actionable intelligence is the identification of ads that identify victims of human sex trafficking. To obtain this actionable intelligence, we created a KM strategy that used the system development methodology. This strategy required a system that applied strong filters to a large unstructured dataset of "women seeking men" ads to eliminate those from genuine individuals. We identified the "women looking for men" section of backpage.com from various southern California cities as our data source. The initial system prototype used an initial ontology of keywords generated from the human trafficking literature as strong filters to demonstrate that it could identify potential trafficking victims. We refined the prototype by using expertise to refine the ontology and by applying text mining/machine learning to verify the ontology of keywords and remove words that all or most ads included. Additionally, we identified that emojis were being used in lieu of

or in addition to keywords. The emoji codes were added to the data analysis. We reapplied the refined ontology (keywords and emojis) as strong filters against a second unstructured dataset to demonstrate again that the system could identify trafficking victims from ads. Also as part of the strategy, we developed processes to extract an unstructured dataset and for applying the strong filters to the unstructured dataset to produce the desired actionable intelligence. In Sections 4.1 to 4.3, we describe how we created these strategy/prototype components.

Creating the Ontology/Keyword Set

To create an ontology/keyword set that could act as strong filters, we used a two-stage process with two different datasets. First, we used the keywords we identified (see Section 2.2) to identify which words from that list were in the first dataset. We extracted the keywords from each ad. To extract ethnic/nationality data, we used keywords in the filter feature of Microsoft Excel from both the text and title columns. We joined the Excel file to an area code location table to determine the origin of the phone number. We individually searched for area codes that the table did not represent online using Google. We used area code information to determine possible movement of providers. In all, 84 percent of the ads produced phone numbers, and we manually extracted another 12.6 percent because the ads disguised the phone numbers in some way. Ads often put random characters between numbers, write out the word, or use letters rather than numbers. Finally, 3.5 percent listed no phone number. We used the resulting list as the ontology/keyword set:

- Movement between cities included:
- **Transient Language:** new in town, just arrived, visiting, in town for the weekend two nights only, new arrival, new arrived, Brand new, limited time
- **Group Work:** Staff, ask for, my friend, sister, we, our, assistant
- Phone number, actual numbers from the dataset (used for three indicators: duplicate phone number, disguised phone number, out of state area code)
- **Restrained Movement:** Incalls only, incall only, only incall, no outcall, contains incall but does not contain outcall
- **Minor Indicators:** Little girl, youthful, sweet, young, college student girl, new in town, fresh, turned 18, only 18, fantasy
- **Unconventional Sex:** Open minded, fetish, kinky
- **Ethnicity:** White, Black, Asian, Islander, Caucasian, African American, Latina, Hispanic, mixed

After reflecting on the first ontology, we realized that the ontology would not be permanent and continue to evolve, especially when the traffickers realized what their words could identify trafficking victims (see Section 5.2.3). Thus, we decided to obtain a second dataset to verify the first stage ontology keyword set and to prototype applying the strong filters using R-based script. We verified the ontology keyword set from the first stage by applying experience from policing and research of human sex trafficking through unstructured interviews with human trafficking experts. Additionally, we used the text-mining module in R to parse the unstructured data to remove stop words and words that all or most ads included. The key issue was discriminating between keywords used in generic solicitations versus those used in marketing victims of human sex trafficking. The impact of these actions resulted in the 9 indicators in the initial ontology being reduced to 6 indicators for the revised ontology. The final ontology is:

- Sale of Services: Donation(s), price, rose(s), dollar(s), jacks, jacksons, hundreds
- **Minor Victims:** Fresh, young, new, tiny, little, new in town, girl, college
- **Ethnicity:** African American: AA, African American, Brown Sugar, Black (Beauty)
- **Asian/Pacific Islander:** Pocahontas, Asian, Pacific Islander
- **Caucasian:** Caucasian, White, European
- **Latina:** Latina, Hispanic
- **Country of Origin/Nationality:** South/East Asia, Eastern/Western Europe, Central America
- **Transient Activity/Movement of Victims:** New in town, just arrived, weekend only, limited time, new arrival, brand new, in town for the weekend, gone, back, leaving soon, only for the weekend, new
- **Non-Independent Worker/Restricted Movement:** Incall only, no outcall, only incalls, come to me, my house

Also, while analyzing the second dataset it was noted that there were emojis in the text and that in many cases the emojis seemed to occur with human sex trafficking keywords. The evaluation of emoji indicators also involved the use of the tm package in R to build a Term-Document matrix with the corpus of ads with each emoji indicator. In order to create a framework for filtering out terms in ads that are not likely to be related to human trafficking, we identified the terms that occurred most frequently across all documents in the corpus to remove from the corpus before analysis. To do this the Term-Document matrix was used to remove sparse terms and then identify the most frequently occurring terms as they are less likely to be specific to human trafficking. These words were selected by identifying not only at the most common terms within the corpus, but also the terms that were present in ads without any indicators of human trafficking. Words common in both these elements were identified as being part of the general ontology for any classified ads related to the provision of sexual services or casual dating and not specific to sex trafficking. For validation of these results, the study looked not only at the most common terms within the corpus, but also the terms that were present in the majority of the documents.

A knowledge management approach was then used to identify emojis in ads likely to be linked to human sex trafficking. Clusters of ads with and without keywords associated with human sex trafficking indicators were built by applying natural language processing methods to the unstructured dataset. These clusters then determined the frequency of the emoji occurring in each cluster. Ad significance was then determined through logistic regression analysis and t and z tests.

Process for Extracting the Unstructured Dataset

We created the first unstructured dataset by scraping Web advertisements from websites known to post sexually explicit solicitations/ads. To make it usable for analysis, we converted the scraped data into a .csv file then manually processed into a Microsoft Excel file for analysis.

After reflection, we obtained the first dataset mostly through a manual process, which we considered unsustainable for an automated system approach, so we decided to create a second dataset to test the revised ontology. As such, we created an automatic Web-scraping tool with various approaches. However, this method did not work well because the target websites blocked automatic Web scraping. As a result, we scrapped the automated Web scraping and repeated the manual process to obtain a .csv file with the raw data. We then processed the raw data file using Excel to remove duplicate postings (in this

study, we analyzed content and not frequency, so multiple postings would bias the results) and to identify records with missing data. We loaded the resulting processed raw data file into R's machine-learning and text-mining functions to remove stop words contained in the English stop word dictionary and to identify words common to all ads.

Process for Applying the Prototype

We developed a simple process that involved actual keyword counts to apply the ontology/keyword set to the unstructured dataset. We used count functions in Microsoft Excel to generate the number of times keywords appeared and to determine if an ad contained a trafficking indicator. We also used other mathematical functions in Microsoft Excel to generate results such as the percentage of ads that contained the keyword.

After reflection, we modified this process for the second prototype. Instead of using Excel to do word counts, we used R to code each add with a series of 0 or 1 codes. R coded each human trafficking victim indicator 0 if an ad contained no ontology/key word indicators or 1 if an ad did contain ontology/keyword indicators. R then summed the number of victim ontology/keyword indicators for each add. By using R to code the dataset, we could automate the analysis portion of the prototype.

APPLYING THE PROTOTYPE

Creating the Dataset

The first application of the prototype used a dataset that we extracted from backpage.com for several cities in California. We chose California because we live in the state and because it is a major hub for prostitution and sex trafficking. California encompasses many ports of entry and lies adjacent to the Mexican border region, which is rife with human trafficking (Goldenberg, et al., 2014).

We gathered data for the study by scraping from the “female escort” section of backpage.com from 11 to 16 February, 2015, across 15 different California cities/counties: Bakersfield, Chico, Fresno, Los Angeles,

Merced, Oakland, Orange County, Sacramento, San Diego, San Francisco, San Jose, San Luis Obispo, Santa Barbara, Santa Cruz, and Stockton. Some errors occurred in the data-scraping process. San Diego only produced about two-and-a-half days of data due to an error, so the data sample for that city was smaller than that for the other large cities. In total, we scraped a total of 5,633 ads. We then processed the data as we discuss in Section 4.2.

After reflecting on the first dataset, we collected the second dataset from the “women seeking men” section of the dating classifieds on backpage.com. The sample included advertisements posted between February and March, 2017, for three major cities/counties in Southern California: San Diego, Los Angeles, and Orange County. We selected this sample because of the close proximity of the three cities, which makes the language used in the advertisements subject to less variability due to regional language differences. The initial dataset included 8,940 records that we processed in accordance with Section 4.2; as a result, 8,744 records remained in the final dataset.

ANALYZING THE DATASET

Analyzing the First Dataset Using the Initial Prototype

We analyzed the first dataset as we discuss in Section 4.3. Specifically, we compiled keywords that indicate possible minor sex trafficking and analyzed them against the advertised age. We combined all ages past 30 into one group as the large majority of ages were between 20 and 25. Note that the advertised ages are not necessarily accurate, especially in trafficking situations. Traffickers may be more likely to advertise a victim of minor sex trafficking as being aged from 20 to 25—young enough to still attract the correct buyer but old enough not to raise law enforcement suspicion. Overall, we found a number of prominent age terms such as “sweet”, “young”, and “fantasy”; rarer terms included “only 18”, “turned 18”, “very young”, and “little girl”. Traffickers would not likely use the rarely used keywords for fear of attracting law enforcement. Additionally, terms such as “college student/girl”, “new in town”, and “fresh”, seem to skew slightly toward younger ages, which could indicate younger individuals.

Many ads had multiple keywords. Out of the sample of 5,633 ads, 4,836 had a least one indicator of human sex trafficking. By far the most prominent indicator was “duplicate phone/ad”. These results are similar to those that Latonero et al. (2012) found. Specifically, these authors found that a small number of phone numbers accounted for a disproportionate amount of ads; however, on reflection, we believe that this disproportion reflects people’s practice of keeping their mobile number even after moving and provides little information with respect to victims of human sex trafficking. As such, we can conclude that a single indicator of human sex trafficking cannot sufficiently identify a potential victim and that duplicate phone/ad by itself does not provide enough discerning information to identify a victim of human sex trafficking but that it is likely to be a good indicator in combination with other indicators. The following list includes the percentage of total ads with the specified indicator present:

- Duplicate ad/phone number (54.8%)
- Ethnicity/national origin (44.9%)
- Unconventional sex (13.4%)
- Disguised phone number (12.5%)
- Out of state area code (12.1%)
- Restriction on movement (11.8%)
- Transient language (9.0%)
- Indications of working in a group (8.8%)
- Minor keyword indicators (5.2%)

The following list shows how many ads had multiple indicators (out of nine indicators):

- 4,836 had at least one indicator
- 3,126 had at least two indicators
- 1,354 had at least three indicators
- 330 had at least four indicators
- 74 had at least five indicators
- Eight had at least six indicators
- One had seven indicators.

Analyzing the Second Dataset Using the Revised Prototype

We analyzed the second dataset as we discuss in Section 4.3.

The following list shows percentage of ads with the indicated keyword indicator:

- Sales of service (1.56%)
- Minor (48.2%)
- Ethnicity (30.3%)
- Country of origin (11.4%)
- Transient language (12.67%)
- Restriction of movement (0.71%)

The following list shows how many ads had multiple indicators (out of 6 indicators):

- 3,534 ads had at least one indicator
- 1,768 ads had at least two indicators
- 467 ads had at least three indicators
- 33 ads had at least four indicators
- Two ads had five indicators

To compare the ontology to the emojis the subset function in R was used to create two populations of ads, one with known indicators of trafficking and the second without indicators of trafficking. These known indicators consisted of keywords/phrases in the ontology used. The indicators of human sex trafficking are: sale of services, minor/underage victims, ethnicity/race, country of origin, transient activity/movement of victims, and non-independent workers/ restricted movement.

- **Ontology Development Identified:** (Note that ethnicity and country of origin emojis are common across all ads and no special emojis were found specific to human sex trafficking)
- **Two Emojis:** The rose and the rosette for the keyword indicator of sale of services.
- **Three Emojis:** The growing heart emoji, cherry emoji, and cherry blossom emoji for the minor keyword indicator
- One emoji, the airplane emoji was the only significant indicator for the keyword indicator of transient activity
- One emoji, the crown emoji was found significant for keywords associated with restricted movement/non-independent.

The following list shows how many ads had multiple emoji indicators:

- 2,237 ads had at least one indicator
- 790 ads had at least two indicators
- 216 ads had at least three indicators
- 36 ads had at least four indicators.

Finally, looking at both keywords and emojis we get the following list having multiple indicators

- 1,825 ads had at least three indicators
- 509 ads had at least four indicators
- 127 ads had at least five indicators
- 37 ads had at least six indicators.

DISCUSSION

It is shown that keywords and emojis can be used as indicators of sex trafficking. It is observed that the number of ads with multiple indicators dropped quickly the more indicators that were identified. This was an expected result that illustrates that the process works. Comparing the number of ads with multiple indicators to the 792 reported cases of human sex trafficking in California in 2015 (NHTRC, 2016) and 544 human sex trafficking cases in the first half of 2017 (Polaris Project, 2017) suggests that one can establish a threshold number of indicators that indicates a possible sex trafficking victim. The first dataset suggests either four or five indicators as the threshold (out of nine indicators). Four is a conservative threshold that will not likely miss any victims but will probably include many false positives on potential victims because, in the sample, 330 ads had four indicators (about 40% of the yearly number of reported sex trafficking cases). Using five or more indicators strongly suggests a victim of sex trafficking: in our sample, five or more indicators yielded 74 potential victims (or 9.3% of the yearly number of reported sex trafficking cases). Given the limited resources available to law enforcement, a more focused number, although it may miss some potential victims, may be better. This logic suggests that four indicators (out of six) in the second dataset as the threshold because 33 ads is about six percent of the 544 cases reported in the first half of 2017. Finally, if using a full ontology including emojis and keywords it is recommended that a threshold of 6 indicators (either emoji or keyword) be used. To sum up, it is recommended that five indicators (when one uses nine indicators total), or four (if one uses six indicators in total), or 6 indicators (if using emojis and keywords) be used as a threshold for recommending law enforcement intervention.

We also observed that, while phone-based indicators seemed to be useful in the first dataset, we removed them from the revised ontology for the second dataset. We removed duplicated phone numbers as an indicator because this indicator did not discriminate between trafficking phone use and regular prostitution phone use well enough. We dropped the other phone indicators (i.e., blocked or disguised phone numbers or out of area phone numbers) because it is becoming too common of a practice to use-fully serve as an indicator (i.e., many people now commonly block or disguise their phone number for privacy and security reasons, and carriers now commonly allow customers to keep their phone numbers when they relocate). Conversely, we have a concern that the indicators do not do a good enough job discriminating between voluntary prostitution and sex trafficking victims. Ethnicity and to a lesser degree country of origin and minor indicators (especially in the second dataset) do not discriminate between sex trafficking victims and voluntary prostitution and only work in conjunction with other indicators, which strengthens the argument for using at least four (when using six in total) or five (when using nine in total) indicators for initiating follow-up actions.

We used backpage.com for this research as a case study, but it only accounts for a portion of all online escort ads. We created a prototype that can be implemented into various websites. The difficulty in using it rests in the data-extraction process as we observed when we attempted to use craigslist.com. It may be possible to use the data-extraction process only when generating/validating the ontology and using the analysis process as a constant online monitoring and alarm tool.

EVALUATING THE PROTOTYPE

The prototype was evaluated by reflecting on the outcomes generated when applying the prototype to a real dataset. As a result, a revised dataset was created and tested. Reflection on these results when compared to outside reports on the numbers of human sex trafficking victims resulted in the recommended thresholds (see Section 5.2.3) to use to identify potential victims of human sex trafficking. Additionally, the system development methodology includes a five-step evaluation process (Burstein & Gregor, 1999) for assessing the quality of the system development methodology process. This assessment is described below. Overall, it is noted that the proposed prototype is acceptable as an output of the system development methodology as it met all steps of the five-step evaluation process.

Significance

Outcomes/artifacts from the system development research methodology should yield significant theoretical contributions, a system that yields better results than those systems currently in use, or both. In our case, we created the latter—a significant practical contribution that yields better results than the ones that currently exist.

Currently, law enforcement agencies search adult service classified ads to find to find pictures of people that look as though they are being trafficked (Latonero et al., 2012). Commonly, law enforcement agencies begin investigating possible sex trafficking by browsing through ads and looking for girls with pictures that look very young. If the girl looks underage, they may open an investigation (Latonero, 2011). They also compare an advertisement's picture with the advertised age. If they perceive a discrepancy between a girl's picture and her advertised age, law enforcement agencies may also open an investigation. Although these techniques have been one way to locate potential victims, they suffer from complications. First, it is extremely tedious and, second, photos are not always accurate (Latonero, 2011). While many law enforcement agencies use these tactics with some success, the system proposed in this chapter may identify more potential victims without generating large numbers of false positives. It is evaluated that the proposed ontology/system has practical significance.

Internal Validity

Internal validity refers to the credibility of one's results and whether they make sense. Established theory was used to generate an ontology that was applied to an unstructured dataset with the results presented in this chapter. The presented results are consistent and expected given the theory used and its application to the problem.

Further, to verify internal validity, rival methods were considered. Other work that has investigated this research area was reviewed, but it has all used some form of ontology-based method for identifying potential victims. For instance, Ibanez and Suthers (2014) used escort advertisement data to evaluate the significance of known indicators of online trafficking activity. They found that ads that contain two or more indicators are more likely to be instances of trafficking and that the most prevalent indicators for trafficking in order are ethnicity/nationality, potential restricted movement, movement along trafficking circuit, and shared management (multiple providers). Dubrawski, Miller, Barnes, Boecking, and Kennedy (2015) trained multiple random forest models using three different information-extraction approaches, termfrequency analysis using law enforcement provided keywords, regular expressions, and machine learning to weight 115 keywords. Alvari, Shakaria, and Snyder (2016) used a sample advertisements

posted on backpage.com in March, 2016, to train a learning classifier. They used a semi-supervised learning algorithm to label the remaining advertisements and had experts in online sex trafficking review the classifications to evaluate accuracy. Considering Alvari et al. (2016), natural language processes and text mining in the prototype were added for the second dataset.

External Validity

External validity concerns “the generalizability of a causal relationship to and across populations or persons, settings, and times” (Burststein & Gregor, 1999, p. 134). To test external validity, the developed prototype was applied across a variety of nationalities and ethnicities but all in the state of California. It is conceded that the prototype can be applied to any population/ad sample in the United States, but it may not be generalizable directly to other cultures. We do believe the indicators are applicable for other cultures and countries, but would need to adjust the ontology to fit their language(s)/culture(s). Using the AI and machine learning approaches incorporated into the second prototype provides a means for identifying and adjusting indicator terms based on language and culture differences. Thus, it is noted that the revised prototype has external validity for the United States and has external validity for other cultures/countries when one adjusts the prototype processes for culture/country.

Objectivity/Confirmability

Objectivity/confirmability concerns ensuring research does not suffer from researcher bias or that the researcher at least reports and discusses them. By basing the indicators on the literature and then generating the ontology by using the words in the extracted data, we removed much of our own bias for our prototype. Further, we used machine learning and text mining in the revised prototype to further reduce it.

Reliability/Dependability/Auditability

Reliability/dependability/auditability concerns quality control. The system was developed using a process that is consistent and stable across researchers and methods. We relied on the literature and the accepted system development research methodology to generate the prototype. Thus, it is concluded the prototype has sufficient reliability, dependability, and auditability.

CONCLUSION

It is concluded that the prototype works and that it deserves further development. We found that the prototype meets the requirements of the system development methodology from action research and that it yields promising results when tested against actual datasets. We also recommend that an alert/warning system be developed based on this research that can provide a warning when ads contain five or more indicators (when using the nine ontology), four or more indicators (when using the six ontology), or six or more indicators (when using emojis and keywords)—thresholds determined based on comparing the number of ads the indicators identified with the number of reported victims (i.e., 792 for the first dataset (NHTRC, 2016) and 544 for the second dataset (Polaris Project, 2017)). We expect the suggest alarm system to result in a low number of positive alarms.

Further, we conclude that the system development method, especially when used with KM, is a viable approach to conducting research into developing systems to solve social problems. We found the method very useful for taking the emphasis off the application of new technologies and keeping the research focused on solving a social problem and building a system to do so.

IMPLICATIONS FOR RESEARCH

The initial prototype is a proof of concept, while the revised prototype moves towards an automated system; however, neither creates any new theory. Research focused on integrating more advanced technologies into a KM system for generating actionable intelligence that authorities can act on could generate significant social benefit. Specifically, we need future research that further focuses on automating the prototype's data-extraction process. A framework for developing the full automated system should be developed based on this research and the framework presented in Jennex (2017), a proposed KM model based on a modified knowledge pyramid.

IMPLICATIONS FOR PRACTICE

Finding victims of human sex trafficking is difficult and requires all the technology innovation possible. The practice of using posted photos and facial recognition is not working well and needs improvement. This study suggests how technology in practice can be used to identify victims of sex trafficking. Practitioners will need to adapt to the processes that we illustrate in the paper and to adapt their intelligence gathering and investigative techniques to take advantage of the technology we prototyped.

LIMITATIONS

This study has two major limitations. First, only female victims were considered. While we recognize that males can also be victims of human sex trafficking, males were not included in the study because we sought only to demonstrate that a KMS could be used to identify victims and considering males made the project more complex than needed.

Second, we cannot prove conclusively that the potentially identified victims were in fact real victims. Given ethical concerns with the research, we could not actively interview rescued victims or actively search for victims.

Both limitations may impact the generalizability of the proposed system but are considered acceptable for this research.

AREAS OF FUTURE RESEARCH

Researchers could extend our findings by investigating at least two areas. First, researchers could examine male victims to determine if the indicators and keywords differ from female victims. Second, they could investigate technologies that can be used to create an automated KMS. We used Excel to conveniently demonstrate a proof of concept in the initial prototype. The second prototype incorporated text mining

and machine learning to assist in automatically generate an ontology and analyze data. Thus, our approach experienced weaknesses in extracting data, and future research needs to develop and automate the data-extraction process.

Additionally, data from online adult service ads can be used to inform the study of the commercial sex industry and, consequently, sex trafficking. The data we gathered shows indications of the geographic trafficking patterns across state borders and the demographic makeup of many individuals. This information can help identify previously unknown trends in sex trafficking.

ACKNOWLEDGMENT

Earlier versions of this research were presented at the 49th and 51st Hawaii International Conferences on Systems Sciences, HICSS, in January, 2016 and 2018. Additionally a journal article version of this paper without addressing emojis was published in Communications of the Association of Information Systems in 2018.

REFERENCES

- Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *Management Information Systems Quarterly*, 25(1), 107–136. doi:10.2307/3250961
- Aldea, A., Banares-Alcantara, R., Bocio, J., Gramajo, J., Isern, D., Kokossis, A., . . . Riano, D. (2003). An ontology-based knowledge management platform. In *Proceedings of the Workshop on Information Integration on the Web* (pp. 7-12). Academic Press.
- Almeida, M. B., & Barbosa, R. R. (2009). Ontologies in knowledge management support: A case study. *Journal of the American Society for Information Science and Technology*, 60(10), 2032–2047. doi:10.1002/asi.21120
- Alvari, H., Shakarian, P., & Snyder, J. E. K. (2016). A non-parametric learning approach to identify online human trafficking. In *Proceedings of the IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data* (pp. 133-138). 10.1109/ISI.2016.7745456
- Amin, S. (2010, January). *A Step Towards Modeling and Destabilizing Human Trafficking Networks Using Machine Learning Methods*. Paper presented at the AAAI Spring Symposium, Stanford, CA. Retrieved from <http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1155>
- Banks, D., & Kyckelhahn, T. (2011). *Characteristics of suspected human trafficking incidents, 2008-2010*. U.S. Department of Justice. Retrieved from <http://bjs.ojp.usdoj.gov/content/pub/pdf/cshti0810.pdf>
- Bouche, V. (2015). A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims. *Thorn Foundation*. Retrieved from https://www.wearethorn.org/wpcontent/uploads/2015/02/Survivor_Survey_r5.pdf
- Boyd, D., Casteel, H., Thakor, M., & Johnson, R. S. (2011). *Human trafficking and technology: A framework for understanding the role of technology in the commercial exploitation of children in the US*. Microsoft Research.

Burstein, F. V., & Gregor, S. (1999). The systems development or engineering approach to research in information systems: An action research perspective. In *Proceedings of 10th Australasian Conference on Information Systems* (pp. 122-134). Academic Press.

Dank, M., Khan, B., Downey, P. M., Kotonias, C., Mayer, D., Owens, C., & Yu, L. (2014). Estimating the size and structure of the underground commercial sex economy in eight major US cities. *The Urban Institute*. Retrieved from <https://www.urban.org/sites/default/files/alfresco/publication-pdfs/413047Estimating-the-Size-and-Structure-of-the-Underground-Commercial-Sex-Economy-in-Eight-MajorUS-Cities.PDF>

Department of Homeland Security. (2014). *What is human trafficking?* Retrieved from <http://www.dhs.gov/definition-human-trafficking>

Dubraski, A., Miller, K., Barnes, M., Boecking, B., & Kennedy, E. (2015). Leveraging publicly available data to discern patterns of human-trafficking activity. *Journal of Human Trafficking*, 1(1), 65–85. doi:10.1080/23322705.2015.1015342

Equality Now. (2017). *Global sex trafficking fact sheet*. Retrieved from <https://www.equalitynow.org/sites/default/files/Equality%20Now%20Sex%20Trafficking%20Fact%20Sheet.pdf>

Goldenberg, S. M., Silverman, J. G., Engstrom, D., Bojorquez-Chapela, I., & Strathdee, S. A. (2014). “Right here is the gateway”: Mobility, sex work entry and HIV risk along the Mexico-US border. *International Migration (Geneva, Switzerland)*, 52(4), 26–40. doi:10.1111/imig.12104 PMID:25346548

Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies*, 43(5/6), 907–928. doi:10.1006/ijhc.1995.1081

Harris, K. D. (2012). *The state of human trafficking in California*. California Department of Justice. Retrieved from <https://oag.ca.gov/sites/all/files/agweb/pdfs/ht/human-trafficking-2012.pdf>

Holsapple, C. W., & Joshi, K. (2004). A formal knowledge management ontology: Conduct, activities, resources, and influences. *Journal of the American Society for Information Science and Technology*, 55(7), 593–612. doi:10.1002/asi.20007

Hovy, E., Bryan, N. M., Philpot, A., Silva, D. R., & Sundararajan, A. (2014). Data Integration from Open Internet Sources and Network Detection to Combat Underage Sex Trafficking. In *Proceedings of the 15th Annual Internet International Conference on Digital Government Research*, (pp. 86-90). New York, NY: Association for Computing Machinery.

Ibanez, M., & Suthers, D. D. (2014). Detection of domestic human trafficking indicators and movement trends using content available on open Internet sources. In *Proceedings of the Hawaii International Conference on System Sciences* (pp. 1556-1565). 10.1109/HICSS.2014.200

Jennex, M. E. (2005). What is knowledge management? *International Journal of Knowledge Management*, 1(4), i–iv.

Jennex, M. E. (2017). Big data, the Internet of things and the revised knowledge pyramid. *The Data Base for Advances in Information Systems*, 48(4), 69–79. doi:10.1145/3158421.3158427

Jennex, M. E., & Bartczak, S. E. (2013). A revised knowledge pyramid. *International Journal of Knowledge Management*, 9(3), 19–30. doi:10.4018/ijkm.2013070102

Juniper Networks. (2014). *Human trafficking in Silicon Valley*. Retrieved from <https://flipflashpages.uniflip.com/3/88537/339160/pub/html5.html#page/1>

Jurisica, I., Mylopoulos, J., & Yu, E. (1999). Using ontologies for knowledge management: An information systems perspective. In *Proceedings of the Annual Meeting-American Society for Information Science* (vol. 36, pp. 482-496). Academic Press.

Latonero, M. (2011). *Human trafficking online: The role of social networking sites and online classifieds*. University of Southern California. Retrieved from https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf

Latonero, M., Musto, J., Boyd, Z., Boyle, E., Bissel, A., Gibson, K., & Kim, J. (2012). *The rise of mobile and the diffusion of technology-facilitated trafficking*. University of Southern California, Center on Communication Leadership & Policy.

Major, M. (2012). *Technology and human trafficking*. University of Idaho. Retrieved from http://www2.cs.uidaho.edu/~oman/CS336/Major_HumanTrafficking.pdf

National Human Trafficking Resource Center (NHTRC). (2018). *NHTRC California state report*. Retrieved from <https://humantraffickinghotline.org/state/california>

National Human Trafficking Resource Center (NHTRC). (2018a). *NHTRC hotline statistics*. Retrieved from <https://humantraffickinghotline.org/sites/default/files/2016%20National%20Report.pdf>

National Institute of Justice. (2012). *Human trafficking*. Retrieved from <http://www.nij.gov/topics/crime/human-trafficking/pages/welcome.aspx>

Noy, N. F., & McGuinness, D. L. (2001). *Ontology Development 101: A Guide to Creating Your First Ontology*. Retrieved from Stanford University website: http://protege.stanford.edu/publications/ontology_development/ontology101.pdf

Nunamaker, J. Jr, Chen, M., & Purdin, T. (1990). Systems development in information systems research. *Journal of Management Information Systems*, 7(3), 89–106. doi:10.1080/07421222.1990.11517898

Operation Broken Silence (OBS). (2012). *The Nashville backpage report: An analysis of the online commercial sex industry and human trafficking in Tennessee*. Retrieved from <http://www.operationbrokensilence.org/wp-content/uploads/2012/01/NashvilleBackpageReport.pdf>

Polaris Project. (2017). *California statistics*. Retrieved from <https://humantraffickinghotline.org/state/california>

Raymond, J. G., Hughes, D. M., & Gomez, C. J. (2001). Sex trafficking of women in the United States. *Coalition Against Trafficking in Women*. Retrieved from http://bibliobase.sermais.pt:8008/BiblioNET/upload/PDF3/01913_sex_traff_us.pdf

Staab, S., Studer, R., Schnurr, H., & Sure, Y. (2001). Knowledge Processes and Ontologies. *IEEE Intelligent Systems*, 16(1), 26–34. doi:10.1109/5254.912382

Varma, V. (2007). Use of ontologies for organizational knowledge management and knowledge management systems. In R. Sharman, R. Kishore, & R. Ramesh (Eds.), *Ontologies* (vol. 14, pp. 21-27). Berlin: Springer. doi:10.1007/978-0-387-37022-4_2

Wang, H., Philpot, A., Hovy, E. H., & Latonero, M. (2014). *Data Mining and Integration to Combat Child Trafficking*. Retrieved from Carnegie Mellon University, School of Computer Science website: <http://www.cs.cmu.edu/~hovy/papers/12dgo-trafficking.pdf>

Wu, J., & Yang, G. (2005). An ontology-based method for project and domain expert matching. In L. Wang, & Y. Jin (Eds.), *Fuzzy systems and knowledge discovery* (vol. 3614, pp. 176-185). Berlin: Springer. doi:10.1007/11540007_22

Yen, I. (2008). Of vice and men: A new approach to eradicating sex trafficking by reducing male demand through educational programs and abolitionist legislation. *The Journal of Criminal Law & Criminology*, 98(2), 653–686.

KEY TERMS AND DEFINITIONS

Emoji: A small digital image or icon used to express an idea, emotion, etc.

Filter: The implementation of KM strategy. A method used to separate the big data, data, information, or knowledge needed to make a specific decision from unneeded big data, data, information, or knowledge.

Human Sex Trafficking: Inducing others to perform a commercial sex act by force, fraud, or coercion; as inducing a person under 18 years of age for such an act; and/or as recruiting, harboring, transporting, providing, obtaining a person for labor or services through the use of force, fraud, or coercion in order to subject them to involuntary servitude, peonage, debt bondage, or slavery (National Institute of Justice, 2012).

Ontology: Knowledge codified by providing a simplified and explicit specification of a phenomenon that one desires to represent (Gruber, 1995; Noy & McGuinness, 2001; Staab et al., 2001).

Human Trafficking and Cyber Laws in Malaysia

Olivia Swee Leng Tan

 <https://orcid.org/0000-0002-5628-6883>

Multimedia University, Malaysia

Rossanne Gale Vergara

Multimedia University, Malaysia

Raphael C. W. Phan

Multimedia University, Malaysia

Shereen Khan

Multimedia University, Malaysia

Nasreen Khan

Multimedia University, Malaysia

INTRODUCTION

The era of digitalization is collectively becoming more of a vehicle for exploitation and criminal activities. That said, transnational criminals are increasingly utilizing the darknet or deep web as a medium for human trafficking. Human trafficking is a global problem and the solution requires a comprehensive response to tackle this borderless crime. In 2018, the U.S. State Department Trafficking in Persons (TIP) Report, ranked Malaysia a Tier 2 Watch List country because the “government of Malaysia does not fully meet the minimum standards for the elimination of trafficking; however, it is making significant efforts to do so”. In Malaysia, women, children, and migrant workers are exploited at every stage of the human trafficking process because of their vulnerability. Especially relevant now is the sophistication of human trafficking in the darknet or deep web. With global society becoming more technologically advanced, traffickers have been able to facilitate much of their criminal activity through technology, which provides both anonymity and access to communication with the entire world (Barney, 2018). That said, cyber laws in conjunction with federal and international laws require constant reviews in order to protect the victims of trafficking. This article reviews the literature on human trafficking, the existing legislations and their effectiveness in Malaysia to combat human trafficking in the internet and deep web. The article analyses the existing policies, Malaysia laws and international laws and instruments that are available to prevent and protect women, children and migrant workers from being trafficked. This article will also suggest the necessary measures to prevent human trafficking in Malaysia.

DOI: 10.4018/978-1-5225-9715-5.ch035

BACKGROUND

3

Human trafficking is often referred to as a modern form of slavery. Furthermore, it is considered a highly lucrative criminal activity and countries with large sex industries create the demand, supply and destination for trafficking in persons. Traffickers often target vulnerable women, children and migrants who seek for better employment and opportunities (Zimmerman & Kiss, 2017). Therefore, it is difficult to draw a line separating trafficking from free choice or voluntary illegal migration or prostitution. Malaysia is a source, transfer and destination country for a significant number of men, women, and children who are trafficked from Indonesia, Thailand, Philippines, Cambodia, Vietnam, Burma, People's Republic of China, India, Nepal, Bangladesh, and Pakistan for sexual and labor exploitation (U.S. Department of State, 2018). Many victims voluntarily migrate to Malaysia to work in factories, construction and agricultural sectors, or as domestic servants, but are later coerced into debt bondage or involuntary servitude (U.S. Department of State, 2018). Currently, the technology growth and use of information and communication technologies (ICTs) have been accompanied by an increase in exploitation and abuse of technology for criminal activities. With regard to cyberspace, the internet is increasingly used by transnational organized criminals for human trafficking (Voronova & Radjenovic, 2016). Trafficking in persons is an obvious form of organized crime that has been affected by the globalized revolution in ICT (Tan, Khan & Abdul Rahim, 2014). Illegal trafficking is not exclusive to sexual exploitation with respect to women or child trafficking, but also covers indentured servitude and child labor (Tan et al., 2014). ICTs such as using the internet and mobile phones are frequently used as a tool for human trafficking since internet control is almost borderless and convenient for human traffickers to operate the trafficking *modus operandi* (Toney-Butler & Mittel, 2018).

The era of digitalization and internet have enabled the organized crime of human trafficking to become more challenging for law enforcement agencies and governments. Law enforcement agencies around the world are largely not prepared for combatting cybercrime due the anonymity of the internet or deep web. The deep web or darknet is considered the hidden part of the internet that cannot be found using traditional search engines such as Google. It can be accessed only via software such as The Onion Router (TOR) without exposing the users' Internet Protocol (IP) address and is used to intentionally hide user identities to participate in illegal trade of guns, drugs, sex, counterfeit money, etc. (Formoso, 2017). Thus, making the internet or deep web alluring for cybercrimes and a vehicle for human trafficking. Furthermore, provide a convenient method for cybersex predators to indulge in their deviant behavior (Plaza, 2015).

Inadequate law enforcement facilitates criminals to exploit victims in the deep web. Due to this flaw, elements of human trafficking can be conducted in the deep web, such as: "exploitation of children for the production of pornographic material, online brides and marriage agencies" (Witting, 2017). Human trafficking in the cyber realm presents devastating legal dilemmas. For instance, because a child posing online conducting sexual acts is considered a victim of child pornography offence. Nevertheless, child pornography offences are often not systematically criminalized under the respective national legislation, which leaves a legal gap and often perpetrators are not charged. Furthermore, prosecutors have considered whether cyber trafficking cases, such as online child sex tourism, can be defined as human trafficking (Witting, 2017).

HUMAN TRAFFICKING

Human trafficking is a spreading and worsening global phenomenon. Women, children and migrant workers are trafficked and exploited worldwide, largely into the sex industry and forced labor. Although approximately 4% of the world's 30.2 million trafficking victims at the end of 2010 were trafficked for sex, those individuals generated approximately 40% of the 96.8 billion in profits generated by human trafficking during 2010 (Bailey, 2018). Data released by the International Labor Organization (ILO) estimated that forced labor in the private economy, including for sexual exploitation, generates 150 billion dollars per year in illegal proceeds (Bailey, 2018). Current global trends in online payment and fast, online information transmission increase the likelihood that human trafficking will only become increasingly profitable in the coming years (Bailey, 2018). While the international community condemns human trafficking and considers its practice unacceptable, trafficking today is stronger and more pernicious than in the past. The causes of trafficking are complex because traffickers are organized crime syndicates. Nevertheless, the main contributing factors of human trafficking include: unequal economic development of countries; adverse impact of globalization processes on less developed countries, which aggravate widespread poverty and inequality; and discrimination and gender based violence perpetrated by patriarchal institutions in societies. Human trafficking is facilitated by: the mobility of people in search of better employment and a better life; the spread of new information technologies; and in the case for sex trafficking, by sexual exploitation becoming more pervasive in every region of the world. Human trafficking is controlled by organized crime and syndicates with multi-layered intermediaries at the local and international levels. The general reasons causing human trafficking are:

1. The devaluation of vulnerable women, children, migrants and discrimination practices
2. The perceived responsibility to support families
3. Lack of educational, employment and vocational opportunities.
4. Globalisation where the rich take advantages of the poor.
5. Lack of laws and enforcement e.g. free trade zone allows free movements and attracts negative forces to the countries.

Criminal syndicates have devised ways to defeat systems set in countries to prevent illegal immigration or human smuggling by incorporating corrupted officials within the country's border control or immigration department. Travel documents provided to victims are authentic through means of the corrupted officials, and other times are counterfeited through technologies. Women, children and migrants sometimes illegally migrate by crossing through several transit countries, making it more difficult to trace them. It is very difficult to trace missing trafficked victims, especially when they possess legal travel documents and the security system at the border control is weak.

The following are definitions of Trafficking in Persons and Smuggling of Migrants according to Malaysia's Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007:

Trafficking in persons means:

all actions involved in acquiring or maintaining the labor or services of a person through coercion, includes the act of recruiting, conveying, transferring, harbouring, providing or receiving a person. (Malaysia Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007).

Smuggling of migrants means:

arranging, facilitating or organising, directly or indirectly, a person's unlawful entry into or through, or unlawful exit from, any country of which the person is not a citizen or permanent resident either knowing or having reason to believe that the person's entry or exit is unlawful and recruiting, conveying, transferring, concealing, harbouring or providing any other assistance or service for the purpose of carrying out the acts mentioned above. (Malaysia Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007).

The magnitude of human trafficking in Malaysia, and the forms of trafficking such as child labor, debt bondage, brides order and sex slave today are more alarming than ever. This “modern-day slavery” surpasses the slave trade of the past in that it has become associated with other criminal activities, such as drug/arms trafficking. Estimates of the number of trafficking activities vary greatly because of the difficulty of data collection for this clandestine activity. Trafficking occurs within countries as well as across national boundaries. The lucrative extent of trafficking and the loose policies to track this organized crime have made it more challenging for the government and non-profit organizations to combat human trafficking in Malaysia.

U.S. STATE DEPARTMENT TRAFFICKING IN PERSONS (TIP) REPORT

The annual Trafficking in Persons (TIP) Report published by the U.S. State Department is a report that ranks all countries from Tier 3 (lowest) to Tier 1 (highest) based on their compliance to the minimum standards set forth in the U.S. Trafficking Victims Protection Act 2000, Div. A of Pub. L. No. 106-386, § 108. The U.S. Trafficking Victims Protection Act (TVPA) attempts to combat trafficking on an international scale together with its annual Trafficking in Persons report. In short, the minimum requirements are:

1. Trafficking in persons are prohibited by the government and is punishable.
2. The punishment prescribed by the government is commensurate with that for “grave crimes, such as forcible sexual assault”.
3. The government should prescribe stringent punishment for anyone with knowledge of “commission of trafficking in persons, to deter and that adequately reflect the heinous nature of the offense.”
4. The government should make “sustained efforts to eliminate severe forms of trafficking in persons”.

The above are known as “the 4Ps”, which under the TIP Report framework, effective anti-trafficking laws are those that:

(1) protect victims, (2) prosecute traffickers, (3) prevent future harms, and (4) utilize community partnerships to combat trafficking.

In determining a country's compliance with these minimum standards, the U.S. State Department considers where countries typically rank in the global supply chain for trafficking (origin, transit, or destination for trafficking); the extent to which government actors were involved or complicit in the trafficking; and what measures are reasonable given a country's economic situation (Bailey, 2018).

MALAYSIA ACCORDING TO U.S. TIP REPORT

In 2011-2013, the U.S. State Department Trafficking in Persons (TIP) Report ranked Malaysia a Tier 2 Watch List country. In 2014, Malaysia was downgraded to Tier 3, which is the lowest grade for countries “not making sustained efforts to comply with the minimum standards to address trafficking” as described in the U.S. Trafficking Victims Protection Act (TVPA). The consequences for countries listed as Tier 3 include denial of non-humanitarian aid, development related assistance and exclusion to enter trade agreements with the United States. In 2015, Malaysia was upgraded to Tier 2 Watch List, which was criticized in the international arena (Renshaw, 2016). The following year, Malaysia maintained its rank of Tier 2 Watch List in 2016. In the 2017 TIP Report, Malaysia was placed at Tier 2; however, because the Malaysia government did not demonstrate overall increasing efforts compared to 2017, the country was again downgraded to Tier 2 Watch List in 2018 because “the government of Malaysia does not fully meet the minimum standards for the elimination of trafficking; however, it is making significant efforts to do so”.

Furthermore, the 2018 TIP Report mentioned that although the Malaysia government “convicted more traffickers, increased criminal enforcement of unauthorized passport retention, granted more victims freedom of movement, tripled funding for NGOs including for three NGO-run shelters, and opened its first trafficking-specific court, and amended its foreign worker levy and Private Employment Agency Act to shift debt burdens away from migrant workers”, the efforts were not enough because it did not “demonstrate overall increasing efforts compared to the previous year”.

According to the 2018 U.S. TIP Report, the Malaysia Trafficking in Persons statistics from 2015-2017 are seen in Table 1 below:

Malaysia’s anti-trafficking efforts may appear less in the 2018 reporting period than its efforts in the previous year; however, in March 2018, the government established an anti-trafficking court for the state of Selangor. The state of Selangor was selected due to its history of having the highest trafficking in persons cases. Moreover, the Malaysia government expanded its directive of interagency law enforcement task force and made it permanent. The task force successfully conducted six operations focused on forced labor in 2017 with the lead enforcement agency as the Royal Malaysia Police. Furthermore, the “Malaysia government conducts or support anti-trafficking trainings, including 34 in-service trainings for police officials and 14 transnational or bilateral trainings in the region focusing on victim protection, law enforcement, and prosecution” (U.S. State Department, 2018).

Even with the above efforts by the Malaysia government, collusion still exists among law enforcement officials with human traffickers i.e. officials accepting bribery in exchange for undocumented border crossing. In 2016, the Malaysia government prosecuted five officials for accepting bribes and four were found guilty for smuggling offenses, while the fifth was acquitted.

The reason for the high potential trafficking victims is because enforcement agencies employed the Malaysia anti-trafficking law broadly by presuming all foreign women during bar or massage parlor raids

Table 1. Malaysia trafficking in persons statistics (2015-2017)

	2015	2016	2017
Trafficking and Tracking Related Investigations	158	581	556
Prosecutions Initiated	38	175	80
Convicted traffickers	7	35	45

Note: From U.S. Trafficking in Persons Report 2018. Retrieved March 30, 2019 from <https://www.state.gov/j/tip/rls/tiprpt/>

Table 2. Malaysia potential vs. confirmed trafficking victims (2016-2017)

	2016	2017
Potential Trafficking Victims	3,411	2,224
Confirmed Victims	1,558	721

Note: From U.S. Trafficking in Persons Report 2018. Retrieved March 30, 2019 from <https://www.state.gov/j/tip/rls/tiprpt/>

as potential victims. The decrease in overall victims identified may be due to the Malaysia government shifting resources toward forced labor vice to their previous focus, which was primarily on sex trafficking (U.S. State Department, 2018).

HUMAN RIGHTS COMMISSION OF MALAYSIA (SUHAKAM)

SUHAKAM is a Human Rights Commission of Malaysia and continues to support the Malaysia government's efforts to strengthen action against trafficking in persons. While Malaysia has laws to criminalize human trafficking, SUHAKAM 2017 Report questions the effectiveness of the implementation of these laws because trafficking in persons continues. In SUHAKAM 2017 Report, human trafficking and smuggling included 12 incidents in Peninsular Malaysia, and 2 in Sabah (SUHAKAM, 2017). Of the 14 cases reported, SUHAKAM addressed that 7 cases were referred to the Anti-Trafficking in Persons and Smuggling of Migrants (ATIPSOM) Task Force, which was established in December 2016, while the rest were not, "due to the lack of substantial information in the complaints as well as the complainants' lack of cooperation to provide further information when requested".

One of the cases referred to the ATIPSOM Task Force was a human trafficking syndicate operating from an apartment in Cyberjaya, Malaysia. Based on a tip off, the task force raided the apartment, arrested the traffickers and rescued five Nigerian women. In another case, the Thailand-based civil society, Alliance Anti Traffic (ATT) informed that they had intercepted the smuggling of two Shan girls in Thailand when they were being enroute from Malaysia to Vietnam. Later was informed that more girls were kept at a location in Ipoh, Perak, Malaysia. On 3 March 2017 based on a tip off, the police rescued 19 Shan girls and a Vietnamese, arrested three suspects and charged them under Section 12 of ATIPSOM on 10 March 2017.

THEORETICAL ASPECT OF HUMAN TRAFFICKING

The first international agreement on the definition of "trafficking in persons" according to the 2000 United Nations Convention Against Transnational Organized Crime Trafficking Protocol Article 3(a) is:

The recruitment, transportation, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. (United Nations, 2000, p. 42).

The term “exploitation” in this definition encompasses: sexual exploitation, forced labor, slavery, servitude and removal of organs. However, this article focuses on human trafficking and cyber laws.

Human trafficking is a form of modern day slavery because trafficked victims are exploited by force or under debt bondage. The point is that, “whilst the practices of trafficking are not central to the global transnational markets or the global world in which we live, as slavery once was, they are nevertheless embedded in the inequalities and injustices of the distribution of wealth promoted and encouraged by the world system” (Santos, Gomes & Duarte, 2010).

Means of Human Trafficking Through Technology/Internet

The means of human trafficking and sex exploitation via technology/internet are frequently used by traffickers due to its borderless recruitment process and larger target of victims around the world. Traffickers are using the internet to advertise their services and force them upon their victims. Craigslist, Facebook and chat rooms specific to these services are not uncommon. Online advertisement has been used by the perpetrator to lure their victims. While, some service providers use their victims to advertising themselves with both real and fake photos to mask under age exploitation. THORN, an NGO co-founded by Ashton Kutcher and Demi Moore to drive tech innovation to fight child trafficking and sexual exploitation reported that 63% of victimized kids are advertised online. The cost of recruitment is lower than the conventional recruitment/trafficked process.

The means of human trafficking through ICT are generally by fraud and coercion or ransom/blackmail. Not only the deep web or darknet are women and children coerced into human trafficking, the internet, where social media is accessed can start the process of human trafficking with a simple flattering comment (Baker, 2019). Such is the case with “Internet Romeos”, whereby traffickers groom their targets by building trust and a relationship with a potential victim. Once the victim is convinced the Romeo is in love, the victim is persuaded to move with him to a new town and manipulates the victim into forced prostitution (Baker, 2019).

The deep web hides your identity and location and may be accessed via a search engine such as TOR. TOR does not retain search engine records and leads the searcher to the desired website without any trace of who they actually are (Jardine, 2015). The dark net also includes assassination services, arms dealing, human experimentation and paedophilia and the means to pay for these service can be anonymous with prepaid debit cards and crypto currency.

Process of Human Trafficking Through ICT

Internet use for sex trafficking victim advertisements such as www.Backpage.com (Backpage) has become increasingly prevalent in recent years due to limited intervention by international government agencies (Kowalski, 2018). Such as the case with the United States government attempting to criminalize advertisements of minors for sex; however is blocked due to U.S. Constitutional challenges, Supremacy Clause, the First Amendment and Commerce Clause (Kowalski, 2018). According to the Thorn organization, victims recently recruited into the sex trade were facilitated by using internet transactions and while the adult section was removed from Backpage in the U.S. market in 2017, purveyors of sex trafficking have found a work around and instead post ads in the dating or massage sections on Backpage. Traffickers have also penetrated general websites such as Facebook to continue on with sex exploitation of women and children.

The process of human trafficking through technology/internet are:

1. Online Chat /Dark Web
2. Recruitment /Process by way of meeting the victims personally
3. The means are usually by force, fraud, coercion or drugs i.e. the push and pull factors in human trafficking.

Traffickers can exploit technology for their own illegal purposes as described above. Prior to the internet, traffickers were forced to reach consumers and conduct business through underground networks. Now, due to the anonymity of the internet or use of the deep web, both traffickers and consumers can conduct business online with minimal risk of being identified. The result is an increased market and consumption in the trafficking in persons industry. Individuals fearful of being identified, and potentially prosecuted for their involvement, can now access information and make connections anonymously from the safety of their own homes.

CYBER LAWS AND SECURITY POLICY IN MALAYSIA

While Malaysia cyber laws were established since 1997, law enforcement is not sufficiently equipped with the specialized knowledge to investigate the borderless nature of the cybercrimes, which continues to increase in Malaysia because there is a significantly lower risk of being detected or prosecuted” (Tan et al., 2014).

Malaysia is one of the earliest nations in Southeast Asia to develop a National Cyber Security Policy and one of the first nations in Southeast Asia to enact cyber laws. The Malaysia National Cyber Security Policy is said to be enacted in 2019. However, at the time of writing this article, Malaysia has not officially enacted its National Cyber Security Policy. The policy’s main objective is to “address the risks to the Critical National Information Infrastructures (CNII) to ensure that they are protected to the level commensurate with the risks they face”.

The policy is aware that the CNII is highly interdependent in nature and the goal of the policy is to establish a comprehensive program that will ensure effective cyber security controls throughout the country’s CNII. According to Jusoh (2016) these CNII assets include “those covering national economic strength, national image, national defence and security, the functioning of the Government and public health and safety”.

In order to combat cybercrime such as human trafficking using Information Communication Technology (ICT), the government of Malaysia amended the Computer Crimes Act 1997 effective as of June 1, 2000 by adding several offenses relating to the misuse of computers to the Act. More specifically, the Computer Crimes Act focuses on “unauthorized access to computer material, unauthorized access with intent to commit other offenses and unauthorized modification of computer contents and makes provisions to facilitate investigations for the enforcement of the Act”.

The Communications and Multimedia Act 1998, which came into effect on the April 1, 1999 “provides a regulatory framework to cater for the convergence of the telecommunications, broadcasting and computing industries, with the objective of making Malaysia a major global center and hub for communications and multimedia information and content services”. The Malaysian Communications and Multimedia Commission (MCMC) was appointed on November 1, 1998 as the sole regulator of the new

Table 3. Internet use, population data and facebook statistics for Malaysia

Population (2018 Est.)	Internet Users (Year 2000)	Internet Users (31 Dec 2017)	Penetration (% Population)	Users % Asia	Facebook 31 Dec 2017
32,042,458	3,700,000	25,084,255	78.3%	1.2%	22,000,000

Note. From “Internet Usage in Asia: Internet Users, Facebook Subscribers & Population Statistics for 35 countries and regions in Asia” by Internet World Stats. Retrieved December 1, 2018 from <https://www.internetworldstats.com/stats3.htm>

regulatory regime. Although regulation in the form of licensing is provided for, one of the cornerstones of the new regulatory framework is self-regulation by the various industries, including the internet and multimedia content industries. The Personal Data Protection Act (PDPA) 2010 was introduced to curb misuse of data to prevent criminal activities.

As discussed earlier in the article, the internet or deep web is alluring for cybercrimes and a vehicle for human trafficking. Moreover, it provides a convenient method for cybersex predators to indulge in their deviant behaviour. This draws attention to the actual number of internet users and the potential of becoming a victim to any form of sexual exploitation. That said, the usage of internet in 2017 for Malaysians age 15 and above was 80.1% (Department of Statistics Malaysia, 2018). This indicates that a tighter regulation of enforcement should be laid in place to curb human trafficking via ICT.

Table 3 shows Malaysia’s internet use, population data and Facebook statistics as of December 31, 2017 according to Internet World Stats.

According to Table 3 the internet penetration of Malaysia has risen by 78.3%, and with 22 million subscribers of Facebook as of December 31, 2017. The 2018 statistic was not available at the time of writing this article; however, at this rate, the statistics above show that there are more internet users in Malaysia and will continue to grow. Thus, Malaysia will need further protection from cyber criminals to feel safer while using their respective ICTs.

CYBERLAWS IN MALAYSIA TO COMBAT TRAFFICKING

Cybercrime is now more lucrative than drug trafficking and online users have the potential to be a cybercrime victim, and in most cases too, its perpetrators, with the younger generation as the most vulnerable targets. Technology is used to cheat, harass, disseminate false information and more than 70% of commercial crime cases in Malaysia are reported as cybercrime cases according to the Royal Malaysian Police (Rapid rise of cyber criminals, 2016, May 20). The existing cyber laws in Malaysia to combat human trafficking in the cyber realm are:

- Computer Crime Act 1997
- Communications and Multimedia Act 1998
- Malaysian Communications and Multimedia Commission (MCMC) Act 1998

However, the above mentioned legislations do not specifically mention human trafficking offenses per se. Instead, each of the Acts can combat human trafficking according to their purposes:

1. Computer Crimes Act 1997 was enacted to “provide for the offenses relating to the misuse of computers” More specifically, to combat human trafficking refer to Computer Crimes Act 1997 Section 4- Unauthorized access with intent to commit or facilitate commission of further offence,

which under Section 4(3) the offender is liable to a fine not exceeding RM150,000 or to imprisonment for a term not exceeding ten years or to both

2. Communications and Multimedia Act 1998 was enacted to:
 - a. To promote national policy objectives for the communications and multimedia industry;
 - b. To establish a licensing and regulatory framework in support of national policy objectives for the communications and multimedia industry;
3. Malaysian Communications and Multimedia Commission (MCMC) Act 1998 was enacted to establish MCMC to “regulate the communications and multimedia activities in Malaysia, and to enforce the communications and multimedia laws of Malaysia, and for related matters”

The current Malaysia legislations’ protection is insufficient to enforce human trafficking through internet. The above legislations provide only a general and broad definitions for prosecuting cyber crimes. The researcher suggest a specific definition for prosecuting “human trafficking” in the cyber laws.

MALAYSIA MULTI-LATERAL EFFORTS TO COMBAT TRAFFICKING

According to U.S. Government Accountability Office (GAO) Report (2018), the U.S. State Department developed international programs to assist countries to include Malaysia to combat trafficking. For instance, in fiscal year 2017, the State TIP Office Project “A cloud-based case data capture, management and analysis platform for anti-trafficking NGOs across Asian countries for standardization of TIP data collection and for data research. The countries involved Malaysia, Cambodia, Burma, Laos, Philippines, Thailand, Bangladesh, India, Nepal, Ghana, Kenya, and Uganda. The project began in October 2014 and ended in September 2018

A second project with State/TIP Office titled Enhancing National Counter-Trafficking Efforts in Malaysia started in January 2016 and ended in December 2017

In September 2015 to September 2019, U.S. Department of Labor/Bureau of International Labor Affairs/Office of Child Labor, Forced Labor and Human Trafficking had a project “From Protocol to Practice: A Bridge to Global Action on Forced Labor (The Bridge Project)” with global priority in Malaysia, Mauritania, Nepal, Niger and Peru; limited activities in Thailand, the Dominican Republic and Paraguay

It is clear that the U.S. and countries to include Malaysia are making efforts to combat human trafficking, however the crime is elusive and continues to be a global issue.

THE PALERMO PROTOCOL IN HUMAN TRAFFICKING

The Palermo Protocol adopted by United Nations on November 15, 2000 to supplement the U.N. Convention Against Transnational Organized Crime, does not take into regard of the possible difference of ‘cyber’ trafficking or ‘offline’ human trafficking, but rather defines human trafficking in article 3 as:

“recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation”

According to Witting (2017) to understand cyber trafficking is to determine whether or not the victim that remained in front of their computer is equally helpless and hence should be considered victims of human trafficking. Furthermore, Witting (2017) says that “many international tools point out that the element of movement is not necessarily required to constitute a human trafficking offense, citing as proof the term ‘harboring’ in article 3 of the Palermo Protocol”. However, in a case where a family member offers their child to strangers to be sexually exploited at home, the family in this case is ‘harboring’ the child for sexual exploitation, and this is considered human trafficking. This shows that the ‘harboring’ person must have received the victim from somewhere, and hence some sort of movement must have taken place earlier. This point has still not been formally addressed under the Anti-pemerdagangan Orang dan Anti-penyeludupan Migran (Malaysia Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007).

To remove a victim from their familiar environment is an integral element of trafficking. Witting (2017) says that:

“In order to facilitate the understanding that even the smallest movement is sufficient for trafficking, the attention was entirely shifted away from the aspect of movement; this simplification might have led to the misconception that no movement is required at all.”

The message that Witting (2017) points out is that “it’s not that a victim has been moved, but rather that the victim has been removed from his or her safe and familiar environment that is the key element in human trafficking.” Hence, this removing of a victim constitutes a form of movement.

FIGHT ONLINE SEX TRAFFICKING ACT (FOSTA) AND STOP ENABLING SEX TRAFFICKERS ACT (SESTA)

In February 2018, President Donald Trump of the United States signed into law “FOSTA” Fight Online Sex Trafficking Act and “SESTA” Stop Enabling Sex Traffickers Act to enable prevention of illegal sex trafficking online. The bills have been hailed by advocates as a victory for sex trafficking victims.

However, the bills have not resolved the “safe harbor” rule of the internet “Section 230 of the 1996 Communications Decency Act”. Section 230 states that “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” This means that under Section 230 it is permitting “the internet to thrive on user-generated content without holding platforms and ISPs responsible for whatever those users might create” (Romano, 2018, April 18).

But FOSTA-SESTA creates an exception to Section 230 whereby “website publishers would be responsible if third parties are found to be posting ads for prostitution including consensual sex work on their platforms”. The goal of this is supposed to police online prostitution rings easier. What FOSTA-SESTA has actually done, however, is create confusion and immediate repercussions among a range of internet sites as they grapple with the ruling’s sweeping language (Romano, 2018, April 18).

Malaysia is advised to foster or model FOSTA-SESTA; however, Malaysia Communication and Multimedia Commission currently has only Anti-trafficking in Persons and Smuggling of Migrants (ATIPSOM) 2017, Computer Crimes Act 1997, Commission Multimedia Act 1998 and the Penal Code to combat human trafficking.

RECOMMENDATIONS

Combatting human trafficking in the digital world is constantly evolving. Prevention efforts need to focus on the intersection of inter-government cooperation, cyber cops and technology.

The following recommendations are recommended to further combat human trafficking through the internet:

1. Online surveys on the use of technology to recruit, groom and sell domestic minor sex trafficking victims should be conducted. This will provide qualitative data on human trafficking.
2. Provide tools for law enforcement agencies in Malaysia and enforcement officers to be trained to handle human trafficking.
3. Government funds should be allotted for combating human trafficking efforts.
4. Advertisements against human trafficking should be placed on search engine results for pornography.
5. Further government collaboration is required for international, national and domestic law, NGO and accountability of internet usage.
6. Include specific definition for prosecuting “human trafficking” in the Malaysia cyber laws.

CONCLUSION

Human trafficking has evolved with the aid of technology, the internet and deep web. Traffickers are actively using the internet as a means to recruit, lure women and children into this heinous crime. Efforts to fight human trafficking as cybercrime are getting more challenging as the culprits are getting more innovative in dark web operations. The challenges of current cyber laws in Malaysia to combat human trafficking is to review the current cyber laws legislations and also to train the officers to handle human trafficking based on the proposed revised cyber laws on human trafficking.

REFERENCES

- Bailey, M. (2018). U.S. Policy on Human Trafficking, A Partial Solution for a Perplexing Global Human Rights Problem. *Indonesian Journal of International & Comparative Law*, (4), 607. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.indjic15.30&site=eds-live>
- Baker, A., Addario, L., Winters, P., & Rhodan, M. (2019). The Survivor. *Time*, 193(3), 36. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edb&AN=134160312&site=eds-live>
- Barney, D. (2018). Trafficking Technology: A Look at Different Approaches to Ending Technology-Facilitated Human Trafficking. *Pepperdine Law Review*, (4), 747. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.pepplr45.25&site=eds-live>

Department of Statistics Malaysia. (2018). *ICT Use and Access by Individuals and Households Survey Report, Malaysia, 2017*. Released March 19, 2018. Retrieved December 1, 2018 from https://www.dosm.gov.my/v1/index.php?r=column/cthemByCat&cat=395&bul_id=bHBzbWxkWEIxRDlmaU81Q3R2ckRkZz09&menu_id=amVoWU54UTl0a21NWmdhMjFMMWcyZz09

Deshpande, N. A., & Nour, N. M. (2013). Sex trafficking of women and girls. *Reviews in Obstetrics & Gynecology*, 6(1), e22–e27. PMID:23687554

Formoso, J. (2017). *Human trafficking on the dark web and beyond*. Retrieved from <http://www.fox5ny.com/news/human-trafficking-on-the-dark-web-and-beyond>

Grover, J. (2018). State and USAID Should Improve Their Monitoring of International Counter-trafficking Projects. *GAO Reports*, 1–78. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=bth&AN=133416819&site=eds-live>

Huling, A. (2012). Domestic Workers in Malaysia: Hidden Victims of Abuse and Forced Labor. *New York University Journal of International Law & Politics*. New York University. *International Law Society*, 44(2), 629. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edb&AN=74646207&site=eds-live>

Jardine, E. (2015). *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Center for International Governance Innovation and Chatham House.

Jusoh, S. (2016). *Cyber Related Policies and Laws in Malaysia*. Retrieved December 2, 2018 from <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-related-policies-and-laws-malaysia>

Kowalski, S. E. (2018). Holding Internet Advertising Providers Accountable for Sex Trafficking: Impediments to Criminal Prosecution and a Proposed Response. *The Boston University Public Interest Law Journal*, 99(1). Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.bupi27.7&site=eds-live>

Malaysia Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007.

Maras, M. H. (2017). Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking? *Journal of Internet Law*, 21(5), 17–21. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=bth&AN=125989017&site=eds-live>

Ndiaye, N. (2002). *International Organisation for Migration Statement*. On the occasion of the Special Session of the General Assembly on Children, New York, NY.

Phinney, A. (2001). *Trafficking of women and children for sexual exploitation in the Americas – an introduction to trafficking in the Americas*. Women, Health and Development Program. Pan-American Health Organization. Retrieved December 2, 2018 from <https://www.oas.org/en/cim/docs/Trafficking-Paper%5BEN%5D.pdf>

Plaza, P. P. (2015). My Mother, My Pimp: Jurisdictional and Evidentiary Issues in Prosecuting Internet-Facilitated Sex Trafficking. *Philippine Law Journal*, 687(4). Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.philplj89.36&site=eds-live>

Rahayu, N. (2017). Indonesian Migrant Worker Policies and the Vulnerability of Women Migrant Workers to Becoming Trafficking Victims: An Overview of Recent Legislation. *Journal of Southeast Asian Human Rights*, (2), 159. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.jseahr1.14&site=eds-live>

Rapid Rise of Cyber Criminals. (2016, May 20). *Star Online*. Retrieved December 1, 2018 from <https://www.thestar.com.my/opinion/letters/2016/05/20/rapid-rise-of-cyber-criminals/>

Renshaw, C. (2016). Human Trafficking in Southeast Asia: Uncovering the Dynamics of State Commitment and Compliance. *Michigan Journal of International Law*, 37(4), 611. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edb&AN=121106877&site=eds-live>

Romano, A. (2018, April 18). *A new law intended to curb sex trafficking threatens the future of the internet as we know it. The controversial bill package FOSTA-SESTA has already impacted sites like Reddit, Craigslist, and Google — and that's just the start.* Retrieved December 4, 2018 from <https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom>

Stop Violence Against Women. (2018). *Trafficking in Women. Stop Violence Against Women: A Project of the Advocates for Human Rights.* Retrieved December 1, 2018 from http://www.stopvaw.org/trafficking_in_women

Tan, O. S. L., Khan, S., & Abdul Rahim, R. (2014). Internet: The double-edged sword of trafficking of women in Malaysia. *Pertanika Journal of Social Science & Humanities*, 22, 149–160.

Toney-Butler, T. J., & Mittel, O. (2018). *Human Trafficking*. Treasure Island, FL: StatPearls Publishing. Retrieved April 1, 2019 from <https://www.ncbi.nlm.nih.gov/books/NBK430910/>

United Nations. (2000). *United Nations Convention Against Transnational Organized Crime*. Retrieved December 1, 2018 from https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

United Nations Office on Drugs and Crime. (2012, July 19). *Human trafficking: organized crime and the multibillion dollar sale of people*. Retrieved December 4, 2018 from http://www.unodc.org/unodc/en/frontpage/2012/July/human-trafficking_organized-crime-and-the-multibillion-dollar-sale-of-people.html

U.S. Department of State. (2018). *Trafficking in Persons Report June 2018*. Retrieved from <https://www.state.gov/documents/organization/282802.pdf>

U.S. Government Accountability Office. (2018). *Human Trafficking: State and USAID Should Improve Their Monitoring of International Counter-Trafficking Projects*. GAO-19-77. Retrieved from <https://www.gao.gov/products/GAO-19-77>

Voronova, S., & Radjenovic, A. (2016). *The Gender Dimension of Human Trafficking*. European Parliamentary Research Service (EPRS). PE 577.950. Retrieved December 4, 2018 from [http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI\(2016\)577950_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI(2016)577950_EN.pdf)

Witting, S. (2017, June). 'Cyber' Trafficking? An Interpretation of the Palermo Protocol in the Digital Era. *Völkerrechtsblog*, 28. doi:10.17176/20170629-162348

Zimmerman, C., & Kiss, L. (2017). Human trafficking and exploitation: A global health concern. *PLoS Medicine*, 14(11), e1002437. doi:10.1371/journal.pmed.1002437 PMID:29166396

KEY TERMS AND DEFINITIONS

Cyber Law: The legal system dealing with cyberspace and the internet.

Darknet: The hidden computer network typically used for illegal trading and forums to include illicit activities such as human trafficking.

Deep Web: The hidden part of the web invisible to conventional search engines.

Human Trafficking: Modern day slavery or illegal transporting of people typically for the purposes of forced labor or sexual exploitation.

Sexual Exploitation: Taking advantage of a person sexually for personal gain or make profit.

Smuggling of Migrants: The facilitating of illegal entry of a person into a country he or she is not a national or resident of.

Trafficking in Persons: Human trafficking or the recruitment, transfer, transportation, or harboring of people by coercion or force, abduction, fraud, deception.

Web-Based Child Sexual Exploitation

3

Lacey Nicole Wallace

Penn State Altoona, USA

INTRODUCTION

Use of technology including smartphones and social media is extremely common among youth. In a 2018 poll by the Pew Research Center, 85% of teens ages 13 to 17 reported that they used YouTube (Anderson & Jiang, 2018). In the same poll, 72% of teens reported using Instagram, 69% reported using Snapchat, 51% reported using Facebook, and 32% reported using Twitter. Use of web-based technology among juveniles increased sharply in recent years. In 2015, about three-quarters of teens had a smartphone or access to a smartphone (Lenhart, 2015). In 2018, more than 95% of teens had a smartphone or easy access to one (Anderson & Jiang, 2018). About 88% had access to a desktop or other form of home computer. Social media use has also evolved. In 2015, Facebook was the most common social media platform used by teens (Lenhart, 2015). In 2018, Snapchat became more popular among teens, though Facebook use remained more common among low-income youth (Anderson & Jiang, 2018). Teens today use a variety of social media and other web-based platforms to communicate, learn more about the world, and entertain themselves (Anderson & Jiang, 2018; Lenhart, 2015). Teens also spend a substantial portion of their time online. In 2018, 45% of teens reported that they were nearly constantly online (Anderson & Jiang, 2018). That figure was only 24% in 2015 (Lenhart, 2015).

Unfortunately, use of social media and other technologies can place teens and other juveniles at risk for sexual exploitation. One example is sexting, a trend that has grown in popularity among youth. Across 39 studies, an average of 15% of juveniles reported sending a sexually explicit text message to someone (Madigan, Ly, Rash, Ouytsel, & Temple, 2018). More than a quarter, 27%, reported receiving a sexually explicit text message. Once sent, juveniles risk having the sext forwarded to other juveniles or adults, or posted online, without their consent. Roughly 12% of juveniles reported forwarding sexts without consent (Madigan et al., 2018). In some cases, commonly termed revenge porn, the forwarded content is used to bully, embarrass, or intimidate the youth involved.

The web can also be used as a tool to engage in other forms of child sexual exploitation, such as child pornography or child prostitution. This chapter explores this topic with the following objectives:

- Define child sexual exploitation and its various web-based forms
- Detail the state, Federal, and international laws prohibiting child sexual exploitation
- Outline what is known about victims and offenders
- Describe current initiatives to prevent or detect web-based child sexual exploitation

Additionally, this chapter describes difficulties in prosecution and detection as well as areas where further investigation is needed.

DOI: 10.4018/978-1-5225-9715-5.ch036

DEFINING CHILD SEXUAL EXPLOITATION

The Federal Bureau of Investigation (FBI) defines the term exploitation as “the act of taking advantage of something; esp., the act of taking unjust advantage of another for one’s own benefit.” Since the definition is vague, many activities involving children (youth under age 18) can be classified as criminal exploitation, including sexual abuse and rape. Many examples in this chapter fall under the category of commercial sexual exploitation of children (CSEC). CSEC refers to sexual exploitation of children for either financial benefit or in exchange for items or services that hold a value of some sort. Examples of CSEC and other forms of child sexual exploitation that can be facilitated through the web include:

- Child pornography production and distribution
- Child prostitution
- Transporting children for the purpose of prostitution (also termed sex trafficking)
- Webcam child sex tourism (WCST)
- Online child sexual exploitation (OCSE)

These terms can be somewhat confusing since countries and other sources sometimes disagree on definitions. Additionally, some forms of CSEC can occur in person while others require no face-to-face contact.

Child Pornography

In the U.S., Federal law defines child pornography as “any visual depiction of sexually explicit conduct involving a minor.” (Department of Justice, 2015c) Child pornography can come in many forms including video, photographs, and computer-generated images designed to look like real children. While the phrase sexually explicit can refer to images of children engaged in sexual activity, that is not a requirement under the definition. Images that are sexually suggestive may also be considered child pornography. Unlike some of the other forms of exploitation, child pornography does not require face-to-face contact between the minor involved and the end-recipient (i.e. consumer). Given available technology, child pornography can easily be obtained and transferred on the web. One example is the increasing prevalence of P2P, or peer-to-peer networks, in the distribution of child pornography. P2P networks are computers connected to each other via the web, where files can be shared directly across computers without the need for a central server (Wolak, Finkelhor, & Mitchell, 2012).

An additional concern is that images later distributed as child pornography may not have been initially intended as such. Revenge porn refers to the use of sexually explicit images without someone’s consent, typically to embarrass, bully, or intimidate. When used to gain money, services, or other items, this behavior is referred to as sextortion. As one example, an adult man in Florida named Michael Chansler contacted at least 350 teenage girls across the U.S. and Canada between 2007 and 2010 and persuaded them to send him sexually explicit images (Greenberg, 2017). Later, he threatened to tell the girls’ parents if they did not continue to send him sexually explicit images. He was later convicted on child pornography charges.

Child Prostitution

The term prostitution refers to participation in any form of sexual activity for profit. In this case, profit can refer to financial gain or the exchange of sexual favors for services or physical goods. For adults, prostitution is illegal everywhere in the U.S. except for certain counties in Nevada (FindLaw, 2018). Even in those counties, however, there are strict restrictions on who can participate and where. Prostitution involving any individual under age 18 is illegal in all jurisdictions in the U.S.. While the term sexual activity may imply that face-to-face contact between a minor and an adult is necessary, attempting to solicit a minor for sexual activity over the internet is also considered a crime.

Child Sex Trafficking

The U.S. Department of Justice (2015b) defines child sex trafficking as “the recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a minor for the purpose of a commercial sex act.” In many instances, the terms prostitution and trafficking are used synonymously when referring to crimes involving children (Montgomery, 2010). Indeed, child prostitution is a form of child sex trafficking since patronizing and soliciting a minor for participation in sexual activity are both included in the definition of child sex trafficking. Yet, child sex trafficking is a broader category of offenses that include both crimes that take place in person as well as those that do not involve face-to-face contact. One example of the latter is webcam child sex tourism.

Webcam Child Sex Tourism (WCST)

Child sex tourism is defined as the “the commercial sexual exploitation of children by people who travel from one location to another and take part in sexual acts with children” (Kapell, 2009, p. 7). Given advances in technology over the past several decades, however, physical travel is no longer necessary for certain forms of this behavior. Webcam child sex tourism refers to adults who pay to watch children engage in sexual activities live via webcam (Acar, 2017). This behavior is also termed webcam child sexual abuse. In some cases, viewers can interact with the children involved and request that they perform specific actions. Often, the viewer and child are in different countries (Terre des hommes, 2018). However, this is not always the case.

Online Child Sexual Exploitation (OCSE)

Webcam child sex tourism is one form of a broad range of offenses termed online child sexual exploitation (OCSE) or online child sexual abuse. These terms refer to the use of information technology including social media, webcams, or cell phones to solicit or coerce children to engage in illegal or inappropriate sexual activity. Since no face-to-face contact is required, these behaviors often do not fit traditional definitions or understandings of child sex trafficking. Often, OCSE is preceded by a behavior known as grooming. Grooming refers to an offender’s efforts to gain a child’s trust and collect information about the child before making sexual advances (Kloess, Beech, & Harkins, 2014).

LAW

Many U.S. laws prohibit the sexual exploitation of children (Adams & Flynn, 2017). These include laws at the state and federal level as well as international agreements to which the U.S. is a party. The pages to follow review key Federal laws as well as examples of law and policy at the state and international level.

Federal

Child exploitation typically falls under Federal jurisdiction if the crime involved individuals in multiple states or countries, if the offense involved the internet, and in some cases where the materials or equipment used in the crime originated in a different state or country than where the crime occurred (Department of Justice, 2015c). At the Federal level, the law (USC § 2251) states that any individual who

employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct (U.S. Government, 1978b)

is guilty of a criminal offense. In other words, this law makes the production of various forms of child pornography illegal. Those outside of the U.S. who commit these offenses are also criminally liable if they transport or intend to transport sexually explicit material involving minors to the U.S. (U.S. Government, 1978b). Transport can include web, phone, or other electronic transfer; it does not need to involve a person traveling to or from the U.S. Penalties for committing these offenses are severe and increase in severity for those who have previously committed crimes involving children. A first offense results in incarceration for 15 to 30 years, a second in a sentence of 25 to 50 years, and a third results in 35 years to life in prison (U.S. Government, 1978b). Additionally, individuals can be prosecuted for knowingly possessing or receiving sexually explicit images of children; both production and consumption of child pornography are illegal in the U.S. (U.S. Government, 1978a).

Federal law (18 USC §2251A) further prohibits buying, transferring custody, or selling children for the purpose of sexual activity (U.S. Government, 1988). Each of these actions is a form of child sex trafficking. As with child pornography production and distribution, penalties are quite severe. The sentence for a first offense is 30 years to life in prison, regardless of whether that person is found guilty of selling a child, taking custody of a child, or purchasing a child for sexual purposes. However, child sex trafficking can involve other activities that extend beyond buying and selling. Under Federal law (18 U.S. Code § 1591), any person who “recruits, entices, harbors, transports, provides, obtains, advertises, maintains, patronizes, or solicits” a person for the purpose of sexual activity is guilty of sex trafficking (U.S. Government, 2000). These behaviors can occur on- and off-line. Penalties for these activities are more severe if they involve children under 14, but also involve a sentence of imprisonment for 10 years or more (U.S. Government, 2000). In addition to the statutes noted above, sex trafficking for both children and adults is prohibited by the 2000 Trafficking Victims Protection Act, the 2015 Justice for Victims of Trafficking Act, and the 2014 Preventing Sex Trafficking and Strengthening Families Act (National Conference of State Legislatures, 2018).

State

3

While child trafficking, prostitution, and pornography prohibitions are also found at the state level, several states have passed additional laws to address child sexual exploitation. Safe Harbor laws are one example. These laws provide criminal immunity to juveniles who have committed criminal offenses as part of their exploitation. Juveniles involved in prostitution, for example, are committing a crime but may be exempt from criminal prosecution. Instead, the adult involved would be prosecuted. As of 2017, 20 states and the District of Columbia had such laws (National Conference of State Legislatures, 2017). There is significant variation in the specifics of these laws. North Dakota, Oklahoma, Kentucky, and Montana, for instance, require proof that a juvenile has been trafficked before the juvenile is eligible for criminal immunity. In Tennessee, criminal immunity is automatically applied if police determine that person involved in prostitution is under age 18. Some states only extend immunity for prostitution while others include additional crimes that may involve trafficking (National Conference of State Legislatures, 2017). Additionally, some states only extend immunity to those under age 16 (Newcombe, 2015).

Another state-level legislative initiative involves diverting youth who have been involved in child sex trafficking to programs and treatments outside of the juvenile justice system. These youth receive social services, counseling, housing assistance, and other aid as an alternative to juvenile justice processing. Generally, diversion is limited to first-time, non-violent offenders. As of 2017, 29 states and the District of Columbia had such efforts in place; 18 states and the District of Columbia offer both diversion and criminal immunity to juveniles involved in sex trafficking (National Conference of State Legislatures, 2017). In New York, as one example, a judge can convert a youth's charge to a person in need of supervision if the youth is 16-17 years old and enters a guilty plea. With this change, the youth is eligible for treatment and services rather than punitive sanctions. In Florida, youth believed to be sexually exploited can be classified as dependents and placed into short-term care facilities under the supervision of the Division of Children and Families (National Conference of State Legislatures, 2017).

While sexting may not be intended as exploitative in many cases, it is illegal in some states. Sexting is generally treated less harshly under the law than possession of child pornography, at least when it consists of images shared between minors. When an image is shared with an adult, child pornography prohibitions may apply. Some states also have laws prohibiting revenge porn. In Florida, for example, it is illegal for a person to

publish a sexually explicit image of a person that contains or conveys the personal identification information of the depicted person to an Internet website without the depicted person's consent, for no legitimate purpose, with the intent of causing substantial emotional distress to the depicted person. (Cyberbullying Research Center, 2018)

Georgia has a very similar statute.

One key legal challenge in comparing state laws and policies is that states differ in how they define the age of consent. Age of consent refers to the age at which a juvenile is believed to be capable of giving consent to engage in sexual activity. Sexual activity involving a youth below the age of consent is illegal. As of 2017, there were 31 states with an age of consent at 16 years old, 8 states where the age of consent was 17 years old, and 11 states where the age of consent was 18 years old (Howe, 2017). However, states vary in whether there are civil or criminal liabilities (or both) for offenders, as well as in whether there are exceptions for individuals who are close in age. Florida law, for example, has an exception for cases

where the juvenile is at least 14 and the offender is no more than four years older (Howe, 2017). Age of consent also varies by country, further complicating cross-national cases.

An additional difficulty in managing cases of web-based sexual exploitation is defining jurisdiction. Victim and offender may reside in different states or countries where laws regulating sexual offenses and age of consent vary. While the Federal government often handles cases like these that occur within the U.S., this is not always the case (Department of Justice, 2015c). Generally, an offense must be prosecuted in the same jurisdiction where it was committed. In practice, however, web crimes have been prosecuted based on where the crime initiated, where the crime continued, where the crime was completed, as well as the location where the impact of the crime was most apparent (Department of Justice, 2015a). Since some of these factors are difficult to determine with web-based crimes, the factors used to determine jurisdiction vary on a case-by-case basis.

INTERNATIONAL LAW AND POLICY

Unless worded otherwise, U.S. law typically does not apply to locations outside of the U.S. As a result, web-based crimes involving a U.S. victim and an offender in another nation may be exceptionally difficult to prosecute; the other nation in question would need to assist or cooperate with the U.S. Not all nations are willing or able to do so. While many nations have passed legislation criminalizing trafficking in persons, including offenses involving children, the number of investigations, prosecutions, and convictions for these crimes remains low in most countries. Generally, countries that have had legislation against human trafficking for a longer period of time, like the U.S., have more convictions for these crimes than countries where legislation is more recent (United Nations, 2016). There remain some countries that have yet to criminalize human trafficking. Several international efforts have focused on encouraging nations to adopt legislation that addresses child sexual exploitation and child trafficking more generally.

In 1996, representatives of 122 countries met in Stockholm, Sweden, to participate in the first World Congress Against Commercial Sexual Exploitation of Children (ECPAT International, 2013). At the time, the focus was on addressing commercial child sexual exploitation in Asia. Indeed, the Congress was first proposed by the non-profit organization End Child Prostitution in Asian Tourism (ECPAT) several years earlier. At the conclusion of the week-long Congress, the nations represented unanimously approved the adoption of an Agenda for Action (ECPAT International, 2013). Among other items, the Agenda stressed the need for cross-national partnerships, raising public awareness, and the development of laws criminalizing child sexual exploitation, whether occurring online or otherwise. While the Congress has been repeated twice since 1996, the agreements resulting from each Congress were non-binding, meaning nations could choose to uphold or disregard any recommendations at their discretion.

The recommendations of each Congress were based, at least loosely, on ideals contained in the United Nations Convention on the Rights of the Child (CRC), an international agreement approved by the United Nations in 1989. As of 2018, the United States remained the only country in the world that had not ratified the agreement. The CRC defines a child as any individual under that age of 18, but also notes that children may be defined as adults at an earlier age depending on a nation's laws. In a series of Articles, the CRC describes the civil, political, economic, health, and social needs and rights of children. The CRC, for example, prohibits capital punishment for children, states that children need to be protected from abuse and exploitation, and mandates that children have a right to be raised by their families (United Nations, 1989). Unlike the agreements resulting from the Congress described above, the CRC is legally binding and enforced by the Committee on the Rights of the Child. In 2000, two

Optional Protocols were added to the initial agreement. The second prohibits child prostitution, child pornography, and the sale of children (United Nations, 2000). As of 2018, this protocol had been ratified by 175 nations, including the U.S., and signed by 9 others. Like the overall CRC, each Optional Protocol is legally binding on nations that choose to ratify it.

VICTIMS AND OFFENDERS

Trends

The exact prevalence of web-based child sexual exploitation is unknown. Underreporting is common for sexual victimization in general. Children, specifically, may be further hampered by whether or not they understand that what has taken place is a crime, fear of punishment, or fear of the offender. Offenses are hard to detect, making tracking difficult even when reports are made. Offenses can occur using a variety of technologies and can involve individuals across multiple countries. Additionally, there is little consensus on the definition of online sexual exploitation.

Recent research in the U.S. found that unwanted online sexual solicitations, cases in which individuals made sexual comments or advances towards youth online, decreased among youth between 2000 and 2010. Across three national, self-report surveys, 19% of youth reported experiencing these sorts of requests in 2000 while only 9% experienced these unwanted communications in 2010 (Mitchell, Jones, Finkelhor, & Wolak, 2013). Additionally, youth became increasingly more likely to report to friends or others when these communications were received (Mitchell et al., 2013). Other research, however, found increases in reports of child sexual grooming, pointing to possible increases in web-based child exploitation (Kloess et al., 2014). Between 2004 and 2013, the number of individuals referred to Federal authorities for involvement in commercial sexual exploitation of children doubled (Adams & Flynn, 2017). Most of these cases involved child pornography. However, the percentages of cases detected through task forces also increased from 2006 to 2009, indicating that improvements in detection and reporting may be contributing to apparent increases (Wolak et al., 2012). As stated in the Introduction, there has been an increase in the percentage of teens who reported forwarding sexts without consent (Madigan et al., 2018). While many of these instances involve juveniles forwarding messages to one another, some cases involve adults.

Victims

Some children are more at risk for web-based sexual exploitation by adults than others. Those at greater risk include (Blue Ridge Thunder, 2018; Kloess et al., 2014; Villacampa & Gómez, 2017):

- Females
- Children 13 to 17 years old
- Children who feel lonely or isolated
- Victims of bullying or abuse
- LGBTQ youth
- Children seeking attention, love, or other forms of affection
- Children who are online frequently
- Children who post many personal details online or engage in other risky online behavior

Victim characteristics can vary by the specific type of exploitation considered and the country in question. The Internet Watch Foundation (IWF), for instance, conducted a study of live-streamed sexually explicit activities involving children, most distributed using webcams. Among the 2,082 images and videos identified, the youth involved most commonly appeared to be females between the ages of 11-13 (Internet Watch Foundation, 2018). These youth, however, differ from those who are solicited by adult offenders through social media or other means (Blue Ridge Thunder, 2018; Kloess et al., 2014; Villacampa & Gómez, 2017).

Offenders

Past research found that offenders of online child sexual exploitation held some characteristics in common (Villacampa & Gómez, 2017; Wolak, Evans, Nguyen, & Hines, 2013). They were more often:

- Male
- Non-Hispanic, White
- Individuals with psychological vulnerability: low self-esteem, loneliness
- Unmarried or not in a long-term relationship

Adults who target children online are generally not pedophiles and are typically non-violent (Kloess et al., 2014). Finkelhor's Precondition Model of child sexual abuse provides a useful way to understand why adults target children online (Howells, 1994). The model points to three pathways:

1. **Emotional Congruence:** The offender may feel they have more in common with children than adults
2. **Deviant Sexual Arousal:** For various reasons, the offender is sexually attracted to children
3. **Blockage:** The offender is unable to satisfy sexual or other needs with adults due to stressful or unusual life circumstances

Existing research identified three types of grooming used by adult offenders in cases that involve sexual abuse or exploitation of children (Craven, Brown, & Gilchrist, 2006). One is termed self-grooming and refers to an offender's efforts to justify and deny either their past behavior or actions they intend to take. The second refers to grooming environment and significant others. If an offender intends to meet the youth in person, for example, the offender may need to learn a parent's schedule or identify meeting places where detection is unlikely.

Grooming a child, the third form of grooming, involves identifying a vulnerable child (Craven et al., 2006). As described under Victims, youth targeted online may be victims of bullying or abuse, lonely, craving attention, or questioning their sexual identities (Blue Ridge Thunder, 2018; Kloess et al., 2014; Villacampa & Gómez, 2017). Youth may indicate their vulnerability by posting their thoughts online, reaching out to others for support, or simply by visiting certain websites or chatrooms. An offender can gain a child's trust online in many ways that include, but are not limited to: posing as a same-age peer, offering support or encouragement, complimenting or praising, discussing non-sexual topics first, discouraging contact with others, sharing "secrets," or making promises. With the exception of promises of love or romance, use of trickery and deception is uncommon. Past studies found that only about 5% of online offenders pretended to be teens when they approached victims online (Wolak, Finkelhor,

Mitchell, & Ybarra, 2008). It was also rare for offenders to hide their interest in sex. Most victims who met offenders in person expected sexual activity to occur.

SOLUTIONS AND RECOMMENDATIONS

In an effort to prevent child exploitation, the United Nations monitors child trafficking and other offenses. In 1990, the United Nations established the Special Rapporteur on the sale of children, child prostitution and child pornography. This group of independent human rights experts investigates violations worldwide and provides advice to the U.N. and specific nations on how to address and improve conditions for children. The Special Rapporteur conducts country visits (by invitation), provides annual reports to the U.N., reports violations to the governments of the nations involved, and works to raise awareness through the media, conference presentations, and other venues. The Special Rapporteur reports violations even to those countries that have not signed or ratified the Convention on the Rights of the Child or its Optional Protocols (United Nations, 1990). Unfortunately, convictions for child trafficking and related crimes have remained fairly stable in recent years, even though more countries have passed legislation prohibiting child sex trafficking and other forms of child sexual exploitation (United Nations, 2016). Thus, legislation alone does not seem to be enough to prevent child sexual exploitation.

Other organizations have developed creative solutions to address web-based child sexual exploitation more directly. Terre des Hommes, a non-profit based in the Netherlands, is one example. In 2013, the organization used a computer-generated girl named Sweetie to locate adults taking part in webcam child sex tourism. Sweetie, playing the role of a 10-year-old Filipino girl, had the ability to speak and interact with web users with the appearance of a real girl. Adult offenders, generally men, would approach Sweetie online and make sexual requests. Afterwards, Terre des Hommes reported the adult offenders to their home countries for potential prosecution. In 2013, more than a thousand adult offenders were identified through Sweetie within a two-month period. The non-profit is currently working on more advanced software, Sweetie 2.0, that countries can implement themselves to detect, investigate, and prosecute webcam child sex tourism (Terre des hommes, 2018).

It is not uncommon for local and state law enforcement agencies in the U.S. to use similar tactics to detect and respond to adults seeking out children online. Rather than use a computer-generated girl, many law enforcement agencies instead create social media profiles and other information online to develop a fictional persona of a child, typically female. When approached by adults online, officers posing as the child interact through chat, email, and text. By arranging to meet or through investigating personal information shared by the offender, adults attempting to exploit children can be apprehended. This approach is not without controversy or difficulty, however. In some countries, such as Singapore, the law requires that a real child be contacted in order for a case to be prosecuted. In the U.S., entrapment is a legal defense. If the defendant can show that police led them to commit a crime they would not otherwise have committed, the defendant may be able to avoid prosecution. Further, not all countries have laws against grooming (Urbas, 2010).

FUTURE RESEARCH DIRECTIONS

Additional research is needed to better understand web-based child sexual exploitation. The prevalence of these offenses is unknown. Existing sources of crime data often focus on one offense, like child pornography, but not others. Part of this difficulty stems from the lack of a consistent definition for what web-based child sexual exploitation entails. Unlike other crime types, these are offenses that are not reported through the FBI Uniform Crime Reports (UCR) program. Even if they were, the UCR only account for crimes reported to police; sexual victimization is frequently underreported. A common source of victimization data in the U.S., the National Crime Victimization Survey, includes respondents ages 12 and older. However, the survey does not enquire about web-based sexual exploitation. The Youth Internet Safety Survey, a national self-report survey of youth, has not been replicated since 2010 (Mitchell et al., 2013). As a result of these concerns, recent trends are unknown or, at the very least, unclear.

CONCLUSION

The term child sexual exploitation refers to a wide array of behaviors that occur on- and off-line. Extensive internet and technology use among teens and other juveniles creates many positive opportunities for education and social connections. However, it also provides a context in which exploitation can occur. Unfortunately, detecting and prosecuting web-based child sexual exploitation is very difficult. Laws differ substantially across states, the Federal government, and across nations. Some laws hold juveniles criminally liable for forms of exploitation that involve criminal activity by the juvenile, like child prostitution. Others provide leniency and offer reduced penalties for crimes like sexting that often involve youth. Few countries have yet to pass legislation prohibiting child sex trafficking and related offenses. However, those that have more recent legislation struggle to detect and prosecute cases that occur. Prosecution is further complicated by questions over jurisdiction and age of consent. Currently, little is known about the exact prevalence of web-based child sexual exploitation. Studies of victims and offenders largely rely on cases that were prosecuted through the courts, meaning they are not necessarily representative of all cases. Yet, several U.S. and worldwide initiative are attempting to prevent and address web-based child sexual exploitation. Some involve legislation. Others, however, are attempting to combat offending on the exact platforms where it occurs, using computer-generated children and live individuals posing as children. Further investigation is needed to assess the effectiveness of these efforts long-term, for both identifying offenders and prosecuting offenders.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

- Acar, K. V. (2017). Webcam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology*, 11(1), 98–109.
- Adams, W., & Flynn, A. (2017). *Federal Prosecution of Commercial Sexual Exploitation of Children Cases, 2004-2013* (No. NCJ 250746). Bureau of Justice Statistics. Retrieved from <https://www.bjs.gov/content/pub/pdf/fpcsecc0413.pdf>
- Anderson, M., & Jiang, J. (2018). *Teens, Social Media & Technology 2018*. Pew Research Center. Retrieved from <http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>
- Blue Ridge Thunder. (2018). *How Online Predators Work*. Retrieved from <https://www.blueridgethunder.com/how-online-predators-work/>
- Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*, 12(3), 287–299. doi:10.1080/13552600601069414
- Cyberbullying Research Center. (2018). *Sexting Laws Across America*. Retrieved from <https://cyberbullying.org/sexting-laws>
- Department of Justice. (2015a). *Prosecuting Computer Crimes. Office of Legal Education*. Retrieved from <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>
- Department of Justice. (2015b, May 26). *Child Sex Trafficking*. Retrieved from <https://www.justice.gov/criminal-ceos/child-sex-trafficking>
- Department of Justice. (2015c, May 26). *Citizen's Guide to U.S. Federal Law On Child Pornography*. Retrieved September 27, 2018, from <https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography>
- ECPAT International. (2013, August 27). *Today is the Anniversary of the First World Congress against the Commercial Sexual Exploitation of Children*. Retrieved from <http://www.ecpat.org/news/today-anniversary-first-world-congress-against-commercial-sexual-exploitation-children/>
- FindLaw. (2018). *Nevada Prostitution and Solicitation Laws*. Retrieved from <https://statelaws.findlaw.com/nevada-law/nevada-prostitution-and-solicitation-laws.html>
- Greenberg, P. (2017). *The Newest Net Threat*. Retrieved from <http://www.ncsl.org/bookstore/state-legislatures-magazine/trends-in-state-policy-news.aspx#The%20Newest%20Net%20Threat>
- Howe, A. (2017, November 8). *Legal Age of Consent in All 50 States*. Retrieved from <https://www.thesurvivoralliance.com/forallies/legal-age-consent-50-states/>
- Howells, K. (1994). Child sexual abuse: Finkelhor's precondition model revisited. *Psychology, Crime & Law*, 1(3), 201–214. doi:10.1080/10683169508411956
- Internet Watch Foundation. (2018). *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse*. Retrieved from <https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf>

Kapell, A. (2009). *Sexual Exploitation of Children in Tourism*. ECPAT International. Retrieved from http://www.ecpat.org/wp-content/uploads/legacy/Child-Friendly_Child%20Sex%20Tourism_2009.pdf

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online Child Sexual Exploitation: Prevalence, Process, and Offender Characteristics. *Trauma, Violence & Abuse*, 15(2), 126–139. doi:10.1177/1524838013511543 PMID:24608540

Lenhart, A. (2015). *Teens, Social Media & Technology Overview 2015*. Pew Research Center. Retrieved from <http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/>

Madigan, S., Ly, A., Rash, C. L., Ouytsel, J. V., & Temple, J. R. (2018). Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. *JAMA Pediatrics*, 172(4), 327–335. doi:10.1001/jamapediatrics.2017.5314 PMID:29482215

Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2013). Understanding the decline in unwanted online sexual solicitations for U.S. youth 2000–2010: Findings from three Youth Internet Safety Surveys. *Child Abuse & Neglect*, 37(12), 1225–1236. doi:10.1016/j.chiabu.2013.07.002 PMID:23938019

Montgomery, H. (2010). Defining Child Trafficking & Child Prostitution: The Case of Thailand Understanding Human Trafficking and Its Victims. *Seattle Journal for Social Justice*, 9, 775–812.

National Conference of State Legislatures. (2017, March 30). *Safe Harbor: State Efforts to Combat Child Trafficking*. Retrieved from <http://www.ncsl.org/research/civil-and-criminal-justice/safe-harbor-state-efforts-to-combat-child-trafficking.aspx>

National Conference of State Legislatures. (2018, June 1). *Human Trafficking Overview*. Retrieved from <http://www.ncsl.org/research/civil-and-criminal-justice/human-trafficking.aspx>

Newcombe, A. (2015). Child Sex Trafficking: Legal Overview | Center on Children and the Law. *Child Law Practice Today*, 34(10). Retrieved from https://www.americanbar.org/groups/child_law/resources/child_law_practiceonline/child_law_practice/vol-34/october-2015/child-sex-trafficking--legal-overview.html

Terre des hommes. (2018). *Sweetie: how to stop Webcam Child Sex Tourism*. Retrieved from <https://www.tdh.ch/en/projects/sweetie-how-stop-webcam-child-sex-tourism>

United Nations. (1989). *Convention on the Rights of the Child*. Retrieved from <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>

United Nations. (1990). *Special Rapporteur on the sale of children*. Retrieved from <https://www.ohchr.org/en/issues/children/pages/childrenindex.aspx>

United Nations. (2000). *Optional Protocol to the Convention on the Rights of the Child*. Retrieved from <https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx>

United Nations. (2016). *Global Report on Trafficking in Persons*. Retrieved from https://www.unodc.org/documents/data-and-analysis/glotip/2016_Global_Report_on_Trafficking_in_Persons.pdf

Urbas, G. (2010). Protecting Children From Online Predators: The Use of Covert Investigation Techniques by Law Enforcement. *Journal of Contemporary Criminal Justice*, 26(4), 410–425. doi:10.1177/1043986210377103

- U.S. Government. (1978a). *Certain activities relating to material involving the sexual exploitation of minors, 18 U.S. Code § 2252 § (1978)*. Retrieved from <https://www.law.cornell.edu/uscode/text/18/2252>
- U.S. Government. (1978b). *Sexual exploitation of children, 18 U.S. Code § 2251 § (1978)*. Retrieved from <https://www.law.cornell.edu/uscode/text/18/2251>
- U.S. Government. (1988). *Selling or buying of children, 18 U.S. Code § 2251A § (1988)*. Retrieved from <https://www.law.cornell.edu/uscode/text/18/2251A>
- U.S. Government. (2000). *Sex trafficking of children or by force, fraud, or coercion, 18 U.S. Code § 1591 § (2000)*. Retrieved from <https://www.law.cornell.edu/uscode/text/18/1591>
- Villacampa, C., & Gómez, M. J. (2017). Online child sexual grooming: Empirical findings on victimisation and perspectives on legal requirements. *International Review of Victimology*, 23(2), 105–121. doi:10.1177/0269758016682585
- Wolak, J., Evans, L., Nguyen, S., & Hines, D. A. (2013). Online Predators: Myth versus Reality. *New England Journal of Public Policy*, 25(1), 1–11.
- Wolak, J., Finkelhor, D., & Mitchell, K. (2012). Trends in Arrests for Child Pornography Possession: The Third National Juvenile Online Victimization Study (NJOV-3). *Crimes Against Children Research Center*. Retrieved from <https://scholars.unh.edu/ccrc/46>
- Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online “Predators” and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. *The American Psychologist*, 63(2), 111. <http://dx.doi.org.ezaccess.libraries.psu.edu/10.1037/0003-066X.63.2.111>

ADDITIONAL READING

- Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior*, 44(1), 45–66. doi:10.1007/10508-014-0270-x PMID:24627189
- Berson, I. R. (2003). Grooming cybervictims: The psychosocial effects of online exploitation for youth. *Journal of School Violence*, 2(1), 5–18. doi:10.1300/J202v02n01_02
- Dombrowski, S. C., LeMasney, J. W., Ahia, C. E., & Dickson, S. A. (2004). Protecting children from online sexual predators: Technological, psychoeducational, and legal considerations. *Professional Psychology, Research and Practice*, 35(1), 65–73. doi:10.1037/0735-7028.35.1.65
- Hillman, H., Hooper, C., & Choo, K. K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review*, 30(6), 687–698. doi:10.1016/j.clsr.2014.09.007
- Leary, M. G. (2007). Self-produced child pornography: The appropriate societal response to juvenile self-sexual exploitation. *Va. J. Soc. Pol’y & L.*, 15, 1.
- Westlake, B. G., Bouchard, M., & Frank, R. (2011). Finding the key players in online child exploitation networks. *Policy and Internet*, 3(2), 1–32. doi:10.2202/1944-2866.1126

KEY TERMS AND DEFINITIONS

Child Pornography: Any visual depiction of sexually explicit conduct involving a minor.

Child Prostitution: A youth involved in sexual activity for profit, whether financial or otherwise.

Child Sex Tourism: The commercial sexual exploitation of children by people who travel from one location to another and take part in sexual acts with children.

Child Sex Trafficking: The recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a minor for the purpose of a commercial sex act.

Exploitation: Taking advantage of someone or something for personal gain.

Grooming: Attempts by an adult to build a child's trust and interest before making sexual advances.

Online Child Sexual Exploitation: Use of information technology including social media, webcams, or cell phones to solicit or coerce children to engage in illegal or inappropriate sexual activity.

Revenge Porn: Sexually explicit images sent or posted without a person's consent; often used to intimidate or embarrass.

Sexting: Sending or receiving a sexually explicit text message.

Sextortion: Use of a sexually explicit image or other sexually explicit material to coerce a person.

Using Luring Communication Theory to Analyze the Behavior of Online Sexual Offenders

Charles R. Crowell

 <https://orcid.org/0000-0002-4337-3726>

University of Notre Dame, USA

Jamie Segerson

University of Notre Dame, USA

Mitchell D. Kajzer

University of Notre Dame, USA

Michael Villano

 <https://orcid.org/0000-0002-5212-326X>

University of Notre Dame, USA

Julaine Zenk

University of Notre Dame, USA

Veronica Wegner

University of Notre Dame, USA

Monica M. Bell

University of Notre Dame, USA

INTRODUCTION

The prevalence of sexual offenders (SOs) contacting children online attempting to engage in sexual exploitation has increased dramatically in recent years likely due to more potential victims and greater offender anonymity in online environments (Davidson & Gottschalk, 2011; Hernandez, 2000). Since its inception in 1998, the National Center for Missing and Exploited Children has received nearly 28 million complaints submitted to their CyberTipline® concerning the online enticement of children for sexual acts with an increase of 150% within the first four months of 2016 (NCMEC, 2018). This startling statistic illustrates just how dangerous online environments are for children, and it underscores the pressing need to identify online SOs so they can be apprehended and prosecuted.

Online anonymity is an enabler for SOs. Suler (2004) described the effects of anonymity as instances of the *online disinhibition effect*, a phenomenon in which people say or do things via the Internet that they would not normally say or do in person. Three key factors involved in this process are *dissociative anonymity*, *dissociative imagination*, and *invisibility*. Dissociative anonymity is the ability for individuals to separate their online personae from their real identities (Suler, 2004). Dissociative imagination is the

DOI: 10.4018/978-1-5225-9715-5.ch037

tendency for people to create separate imaginary online personae, allowing them to avoid responsibility for what happens online because they believe it has nothing to do with offline reality (Suler, 2004). Finally, invisibility is the capability to stay hidden from others on the Internet, which is thought to give people the courage to do things they normally would not do (Suler, 2004).

The problem to be addressed in the present study was to examine the viability of a novel approach to the identification of online SOs despite their attempts to hide behind the curtain of anonymity. Specifically, we tested the hypothesis that Luring Communication Theory (LCT) may provide a useful way to understand and identify the steps SOs utilize in their efforts to exploit children using online communications.

BACKGROUND

Differences in the Etiology of Sexual Offending

Considerable past work has indicated that people become SOs in different ways and for different reasons. Building on the earlier work of Finkelhor and Araji (1986), who provided a comprehensive explanation for sexually deviant behavior, Hall and Hirschman (1991), Ward and Siegert (2002), and Middleton, Elliott, Mandeville-Norden, and Beech (2006) all have proposed models of sexual deviancy based on the influence of specific psychological and physiological contributing factors, such as cognitive distortions, difficulties with emotional regulation, personality problems, deviant triggers for sexual arousal, and intimacy deficits, all of which may lead to a distorted understanding of what defines appropriate sexual behavior, a condition sometimes referred to as having a *deviant sexual script*. According to these models, not all of the same contributing factors necessarily need to be present or even dominant for individuals to become SOs. This variability across individuals in the specific factors that can result in the emergence of sexual deviancy means that there are different etiologies, or experiential pathways, for becoming an SO. However, as noted by Middleton et al. (2006), when multiple factors are present simultaneously in an individual, they may develop the *pure pedophile* deviant sexual script in which there is a strong, if not exclusive, preference for children as sexual partners. These SOs gravitate toward online environments because of the greater number of potential victims and the aforementioned anonymity these situations provide (Davidson & Gottschalk, 2011; Suler, 2004).

A Motivational Dichotomy in Online Sexual Offending

The varied factors and pathways by which individuals become sexual offenders likely imply that not all *pure pedophiles* have the same exact deviant sexual scripts. An important study by Briggs, Simon, and Simonsen (2011) revealed two distinct behavioral patterns of online SOs based on an apparent difference in their motives for initiating contact with potential victims. In one pattern, offenders were motivated by the desire to arrange an in-person meeting in order to engage in an offline sexual relationship. These so-called *contact-driven* offenders engaged in a relatively short online relationship with few sexual behaviors because their focus appeared to be on meeting the child without delay (Briggs et al., 2011). In contrast, a second behavioral pattern was exhibited by offenders who were motivated to develop a purely online sexual relationship with their victims, engaging only in cybersex and exhibitionism. These so-called *fantasy-driven* offenders worked to maintain their online relationships for longer periods of time and were not interested in offline contact (Briggs et al., 2011).

Two recent studies provided further insight into the features that distinguish contact- and fantasy-offenders (Chiu et al., 2018; DeHart et al., 2016). Like the Briggs et al. (2011) study, these investigations found that the interactions between fantasy-offenders and their victims tended to be prolonged, often lasting for months; in comparison, contact offenders engaged in brief interactions sufficient to arrange a *hook up*. One reason that contact offenders kept their interactions short was because of concerns regarding the presence of a monitoring guardian who might terminate the contact or thwart the offender's goal of offline contact (Chiu et al., 2018). DeHart et al. (2016) also found that fantasy offenders were more likely than contact offenders to sexually expose themselves to victims by sending digital images. Additionally, nearly half of the fantasy offenders studied by DeHart et al. (2016) sought sexually explicit photos of their victims, whereas less than a quarter of contact offenders requested such images. Further, the study showed that many fantasy offenders would ask their victims about their genitalia and would often attempt to coach victims in methods of masturbation. In contrast, contact offenders sought to confirm the emotional immaturity of their victims in order to identify the viability of further interaction opportunities both online and in person (DeHart et al., 2016). Finally, Chiu et al. (2018) found that contact offenders oftentimes shared their experiences and emotions with their child victims, encouraging them, in turn, to open up. This strategy helped contact offenders build trust, which made in-person contact with their victims more viable.

Online Sexual Offending and a Luring Communication Process

Clearly, the exploitation goals of online sexual offenders depend on communication with their victims (Aslan, 2011; Black, Wollis, Woodworth, & Hancock, 2015; Whittle, Hamilton-Giachritsis, Beech, & Collings, 2013). A pioneering study reported by Olson, Daggs, Ellevold, and Rogers (2007) used published accounts of interactions between offenders and their victims to examine the communication processes offenders employed to entice their victims. The results of this study revealed a five-step communication process: Gaining Access, Developing Deceptive Trust (DDT), Grooming, Isolation, and Approach. This process, which Olson et al. (2007) referred to as *luring communication*, began with steps to obtain contact with a child-victim followed by multiple steps to engender a cycle of entrapment, luring the child into accepting online sexual advances.

As noted by Whittle et al. (2013), self-disclosure is essential for forging the relationship between offender and victim, and this process is a key part of each step in luring communication (Olson et al., 2007). Self-disclosure has implications for the nature of offender's use of DDT and Grooming, as potential victims will be more likely to disclose personal information if preceded by information about the offender (Chiu et al., 2018; Dindia, 2002). Additionally, Dindia (2002) found a causal relationship between the tendency of individuals to self-disclose and positive feelings toward them on the part of those to whom they disclose—self-disclosure increased positive feelings. By sharing information with and soliciting information from potential victims, SOs are thus able to generate a sense of trust and increase their likelihood of maintaining a relationship.

Elaboration of the LCT has involved adding sub-steps within several of the five major steps for the purpose of more accurately capturing the behavior of online SOs (Kontostathis et al., 2009). For example, within the second step, DDT, Kontostathis et al. (2009) added several sub-steps to better reflect the strategies they observed offenders using within this stage of chat communication. Olson et al. (2007) subdivided several of the later steps based on the analysis of the offender-child dialogues they examined. Considering the number of steps and sub-steps proposed to date (12), the LCT consists of

the comprehensive framework shown in Table 1 for understanding the strategies that SOs use when sexually engaging children.

Using Chat Dialogues to Differentiate Offenders and Victims

Most of the luring communications used by online SOs occur in the context of Internet chat rooms or text-based communications. Examination of these communications is a labor-intensive task that must be carefully carried out by Law Enforcement (LE) as part of identifying and prosecuting Internet predators. Researchers have had to devise ways to expedite the process of offender identification through after-the-fact examinations of chat dialogue transcripts using keyword searches and other text analysis strategies (Kajzer et al., 2018). Pendar (2007) used automatic text categorization techniques to discriminate between online SOs and pseudo-children, who were adult volunteers from Perverted Justice (PJ) posing as children online. Through the use of machine learning techniques focusing on specific word-level trigrams (any set of three words within a chat corpus), Pendar (2007) was able to distinguish between offenders and pseudo-children 94.3% of the time. Using a codebook and dictionary based on the steps in the LCT, Kontostathis (2009) and McGhee et al. (2011) conducted studies using a software application called ChatCoder to analyze chat transcripts via eight coding categories. The researchers were able to distinguish between predator and victim, using chat transcripts from PJ. A success rate of 60% correct identification was found suggesting that the LCT was a useful basis for developing offender identification algorithms that could be implemented in text-analysis software (Kontostathis, 2009). Kajzer et al. (2019) reported a greatly enhanced correct identification rate (>90%) both for offenders vs. victims as well as for offender types (contact vs. fantasy offenders) through the use of word-level models based on chat dialogue text.

Table 1. Luring communication Theory: Five main steps and corresponding sub-steps numbered in sequence from 1-12

Main Steps	Sub-steps				
<u>1. Gaining Access</u> Access to victims	No Sub-steps; only main step Gaining access to potential victims				
<u>Development of Deceptive Trust</u> Developing the relationship	<u>2. Activities</u> Non-sexual activities	<u>3. Compliments</u> Offering praise	<u>4. Personal Information</u> Personal details	<u>5. Relationship Details</u> History and attitude towards relationships	<u>6. Gifts</u> Offering or sending gifts
<u>Grooming</u> Preparing for sexual behavior	<u>7. Communicative Desensitization</u> Sexual language used to desensitize the child			<u>8. Reframing</u> Presenting sexual activity as positive and beneficial	
<u>Isolation</u> Isolation from support network	<u>9. Mental Isolation</u> Providing sympathy and support to the child			<u>10. Physical Isolation</u> Encouraging hiding of the relationship	
<u>Approach</u> In-person meeting	<u>11. Verbal Lead Ins</u> Request to meet for sexual activities			<u>12. Physical Contact</u> In-person meeting for sexual activities	

Note: The first step has no sub-steps

THE PRESENT STUDY

The present study represents a novel investigation in several important respects. First, this study considered all 12 steps and sub-steps of the LCT to classify offenders. Previous classification guided by the LCT has employed this theory on a more limited basis (Kontostathis et al., 2009; McGhee et al., 2011). Second, although several papers cite differences between contact- and fantasy-SO's (Chiu, et al., 2018; McCarthy, 2010; McManus, Almond, Cubbon, Boulton, & Mears, 2016; Merdian, et al., 2018), the present study is unique in its utilization of the LCT to further distinguish between the two offender types. Finally, past studies of online SOs have only been able to use transcripts from PJ. The current study utilizes PJ transcripts along with transcripts of chats between offenders and LE officers posing as children. The chat conversations of undercover LE officers are not generally available and, therefore, have not often been used in previously published research. Use of this data in this study will extend the present findings beyond the single source of chat data currently available to most researchers.

Based primarily on the differences between contact- and fantasy-driven SOs reported by Briggs et al. (2011), several predictions can be made about the outcomes of the present study with respect to luring communication. First, if contact-driven offenders are motivated primarily by the desire to make offline personal contact with potential victims, it follows that these predators should engage in more actions related to Physical Isolation (sub-step of Isolation), Verbal Lead-Ins, and Physical Contact (sub-steps of Approach) compared to fantasy-driven SOs. Second, if fantasy-driven offenders aim to fulfill their desires online, then they might engage in more luring communication behaviors related to developing and maintaining an online sexual relationship with the victim, particularly those involving Compliments (sub-step of DDT), Communicative Desensitization, and Reframing (sub-steps of Grooming) compared to contact-driven SOs. Finally, it could be expected that total number of chat sessions, along with the total length of the online contact, might favor fantasy-driven offenders who are not interested in offline relationships and who, therefore, may be motivated to maintain online contact for as long as possible.

Method

Participants

In this study, chat data was analyzed from two separate sources. First, transcripts of offenders who chatted with civilian vigilante volunteers posing as children online were acquired from the website Perverted Justice (www.perverted-justice.com; PJ). Second, chat data was also analyzed from offenders who had engaged online with undercover police officers posing as children obtained from the office of the St. Joseph County, IN, Prosecuting Attorney. From these sources, researchers randomly sampled and downloaded 33 transcripts from PJ (45%) and 40 transcripts from LE (55%) for a total of 73 transcripts. Each transcript contained a full record of the chat conversations between a single offender and a single pseudo-child.

The number of chat sessions for each offender ranged from one to 14 ($M = 3.32$, $SD = 2.94$). All 73 of the offenders (100%) were male. The offender ethnic makeup was comprised of 64 White (88%), four Hispanic (5.5%), four African American (5.5%), and one Asian (1%). Of these 73 offenders, eight had sexual screen names (11%), while 65 did not (89%). This data consisted of digital evidence from Internet crime investigations that were conducted between the dates of January 1, 2003 and December 31, 2008. All of the chats (100%) were done via Yahoo messenger. In the case of LE chats, the LE officer created a profile of a 13-year-old girl and entered a normal Yahoo chat room, such as "Indiana:1."

While in the chatroom, the officer would not actively engage in any conversation. Rather, an offender would see the pseudo-child enter the room and, if interested, initiate contact through Yahoo messenger.

Offender Classification

For each transcript, the offender was classified by human judges as either a contact-driven or a fantasy-driven offender. Experimenters had knowledge of the disposition of the investigation for the LE chats and knew if the offender had met the pseudo-child in person or had maintained a relationship solely on the computer. The validity of these classifications was checked independently by individual coders. At the completion of the coding process for each chat, an experimenter blind to the disposition classified the offender as either a contact-driven or a fantasy-driven offender. These classifications were then verified against the classifications determined from the disposition of the LE investigation. This verification process resulted in no discrepancies between the LE classifications and the coder classifications.

For the PJ chats, each transcript was initially read by two research assistants. Based on the content of the chat, the offender was classified as either a contact-driven or a fantasy-driven offender. Validity for these classifications was checked by comparing the classifications provided by the two experimenters. Throughout this process, there was 100% agreement. Overall, for both the LE chats and the PJ chats, 39 offenders (53%) were classified as contact-driven offenders and 34 offenders (47%) were classified as fantasy-driven offenders.

Procedure

Luring Communication Theory coding entailed categorizing every line of each transcript sent by the offender (each line was a separate communication or utterance in the messaging system) as belonging to one of the 12 sub-steps of the LCT process, or as being unrelated to any of the LCT categories. This coding was done by two separate coders, blind to each other's classifications. After both codings were completed, the separately coded transcripts were compared for purposes of reliability. The total number of ratings as well as the number of agreements and disagreements between coders were calculated, and inter-rater reliability was calculated using Cohen's Kappa. A Kappa of 0.60 is generally considered to be a moderate level of agreement (Cohen, 1960), and this value was used as the minimum threshold for inter-rater agreements in this study. For the 73 transcripts, Cohen's Kappa ranged from 0.61 to 0.98, with a mean inter-rater reliability of 0.83. These transcripts were then coded by an independent third rater who clarified any disparate codes between the first two coders.

After coding was complete, the original transcripts were examined to determine the number of offender utterances (lines) within each of the 12 sub-steps of the LCT, along with a total of the number of utterances (lines) unrelated to the LCT. This process was done by classifying each coded offender utterance with the number of the sub-step it coincided with (1-12). The total number of utterances made by the offender as well as the utterances that were not categorized into any of the sub-steps were also tallied. For verification, the total number of utterances in all 12 sub-steps as well as those in none of the sub-steps were combined to ensure that this sum equaled the total number of utterances tallied. This check confirmed that every offender utterance was classified as either being in one of the 12 steps of the LCT or not contained in a step. Once a count was obtained, a new variable was calculated that reflected the percentage of utterances made by the offender that were contained in each of the steps of the LCT. The resulting variable thus reflected the percentage of messages sent by an offender for each step of the LCT during the sexual solicitation of the pseudo-child.

Results

Data Exclusions and Analysis Plan

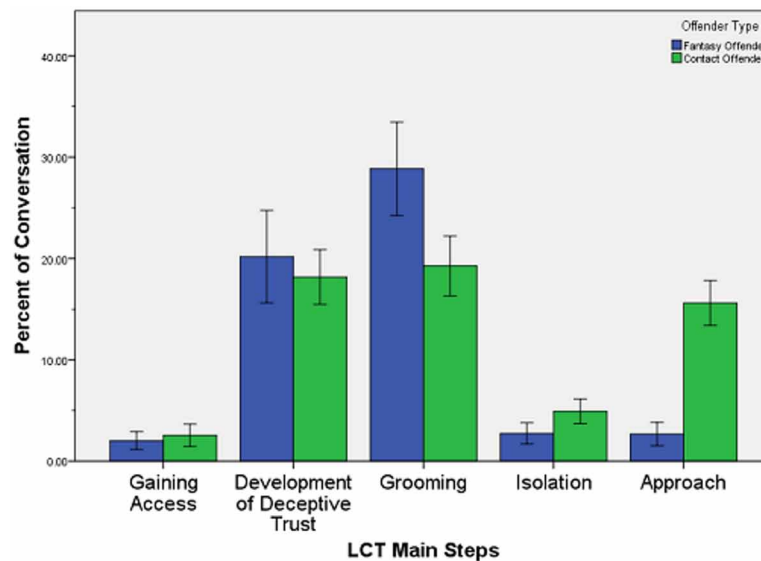
As noted above, each utterance (line) from an offender in each transcript was assigned a code based how the intent of the words in the line related to the steps/sub-steps of the LCT process shown in Table 1. Typically, lines that had relatively few words and/or were not expressing clear thoughts or intentions were coded as unrelated to the LCT. Since the purpose of this study was to examine how the LCT process related to offender communications, lines unrelated to the LCT were excluded from the analyses reported below. While lines unrelated to the LCT accounted for approximately 40% of the total offender *lines* across all chat transcripts, this percentage did not differ across offender types. Moreover, these non-LCT lines represented only a small percentage of the total *words* used by offenders in their communications (approximately 20% of total words). The effects of the independent variables in this study, Offender Type (contact- vs. fantasy-driven) and the LCT main step or sub-step, were assessed by means of mixed-factor ANOVA analyses using Offender Type as a between-subjects factor and the LCT main step or sub-step as a within-subjects factor. Effect sizes were computed as *r* values, where 0.1 is a small effect, 0.3 is a medium effect and 0.5 or above is a large effect (Cohen, 1988). Pooling PJ chats with those from LE was justified in this study by a preliminary analysis involving a Chat Source (PJ vs. LE) by Offender Type by LCT Steps/Sub-steps ANOVA that failed to reveal any significant main effects or interactions of these factors.

The Five Main Steps of LCT

Initially, researchers examined all codes subsumed by the five main steps of the LCT process shown in Table 1. Figure 1 depicts the percentage of offender conversation spent in each of these steps for both contact- and fantasy-driven offenders. It is clear that both types of SOs utilized the steps of DDT and Grooming much more than the steps of Gaining Access and Isolation in their conversations. Offender types differed markedly in their use of Grooming and Approach, but in opposite ways. That is, fantasy-driven offenders used the Grooming step more than contact-driven offenders, whereas the reverse was true for the Approach step.

To confirm these visual impressions, a 2 (Offender Type) X 5 (LCT Category) ANOVA was conducted on the percentage of conversation associated with each main LCT step. The analysis revealed a significant main effect of LCT Category, $F(4,71) = 115.24, p < .001, r = 0.79$, but no main effect of Offender Type. However, the interaction between Offender Type and LCT Category emerged significant, $F(1,71) = 20.86, p < .001, r = 0.47$. Follow-up, between-group tests revealed that the interaction occurred because fantasy-driven offenders engaged in significantly more Grooming, $t(71) = 3.65, p < .001, r = 0.40$, than contact-driven offenders, but significantly less Isolation, $t(71) = -2.69, p < .05, r = 0.30$, and Approach, $t(71) = -10.1, p < .001, r = 0.77$. Pairwise, within-group comparisons across steps within each offender type revealed that, for fantasy-driven offenders, DDT was significantly different from Grooming ($t(33) = 2.54, p < .05, r = 0.40$), and both of these steps were different from each of the remaining steps, all p 's $< .05$, which did not differ from one another. However, for contact-driven offenders, DDT, Grooming, and Approach did not differ, but each differed from both of the remaining steps, all p 's $< .05$.

Figure 1. Percentage of the conversation that contact-driven offenders and fantasy-driven offenders spent in each of the five main steps of the luring communication theory



LCT Sub-Steps

Development of Deceptive Trust

Sub-step comparisons were examined separately for main steps 2-5 (i.e. excluding Gaining Access which did not have sub-steps) starting with the five sub-steps of DDT. Examination of the mean percentage of conversation spent in each of these five sub-steps for each offender type revealed that Personal Information was the most prevalent sub-step used in this category by both offender types while Gifts was the sub-step least utilized. Use of each sub-step did not appear to differ by offender type. A 2 (Offender Type) X 5 (Sub-steps) ANOVA provided statistical confirmation of the impressions gained from examination of the means across the five sub-steps of DDT. The only effect to emerge significant from the analysis was the main effect of Sub-steps, $F(1,71) = 25.59, p < .001, r = 0.51$. Pairwise comparisons revealed that each sub-step was significantly different from all other sub-steps, all $ps < .05$, with the exception of Activities and Compliments, which did not differ from one another. Offender types did not differ for any sub-step.

Grooming

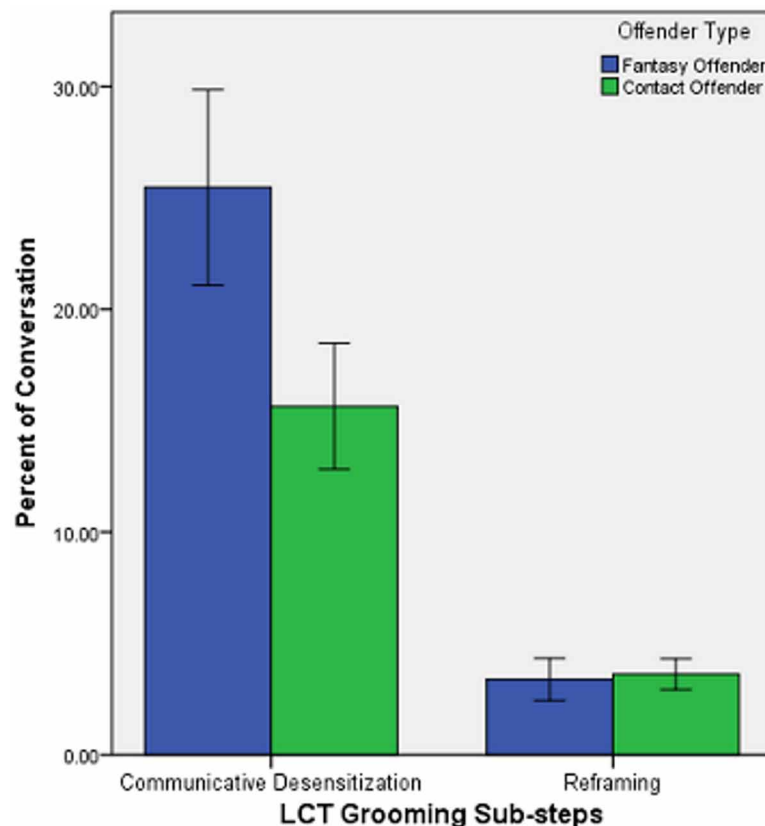
Figure 2 depicts the percentage of conversation spent in each of the two Grooming sub-steps. This figure shows that the first sub-step of Communicative Desensitization (sexual language used to desensitize the child-victim) was used more often during conversations than the second sub-step of Reframing by both offender types. However, fantasy-driven offenders used the first sub-step in this category markedly more than did contact-driven offenders, whereas the two offender types did not appear to differ in their use of the second sub-step. Confirming these visual impressions, a 2 (Offender Type) X 2 (Sub-steps) ANOVA revealed significant main effects of Offender Type, $F(1,71) = 13.34, p < .001, r = 0.40$, and Sub-steps, $F(1,71) = 183.23, p < .001, r = 0.85$, along with the interaction between Offender Type and Sub-steps, $F(1,71) = 15.92, p < .001, r = 0.43$. Follow-up comparisons revealed that the interaction

was due to a significant difference between Offender Type for Communicative Desensitization, $t(71) = 3.91, p < .001, r = 0.42$, but not for Reframing. Fantasy-driven offenders engaged in significantly more Communicative Desensitization than contact-driven offenders. Moreover, paired comparisons showed that both offender types used the first sub-step more than the second (fantasy-driven offenders, $t(33) = 10.27, p < .001, r = 0.87$; contact-driven offenders, $t(38) = 8.46, p < .001, r = 0.81$).

Isolation

Figure 3 depicts the percentage of conversation spent in each of the two Isolation sub-steps. This figure shows that contact-driven offenders used both sub-steps more often than fantasy-driven offenders. Moreover, the difference between offender types in their usage of Mental and Physical Isolation appeared roughly equivalent for both sub-steps. These observations were verified by a 2 (Offender Type) X 2 (Sub-steps) ANOVA showing only a significant main effect of Offender Type, $F(1,71) = 7.26, p < .05, r = 0.30$. Follow-up comparisons revealed that there were significant differences between Offender Types for Mental Isolation, $t(71) = 2.00, p < .05, r = 0.23$, and Physical Isolation, $t(71) = 2.57, p < .05, r = 0.29$. Contact-driven offenders engaged in significantly more Mental Isolation and Physical Isolation than did fantasy-driven offenders.

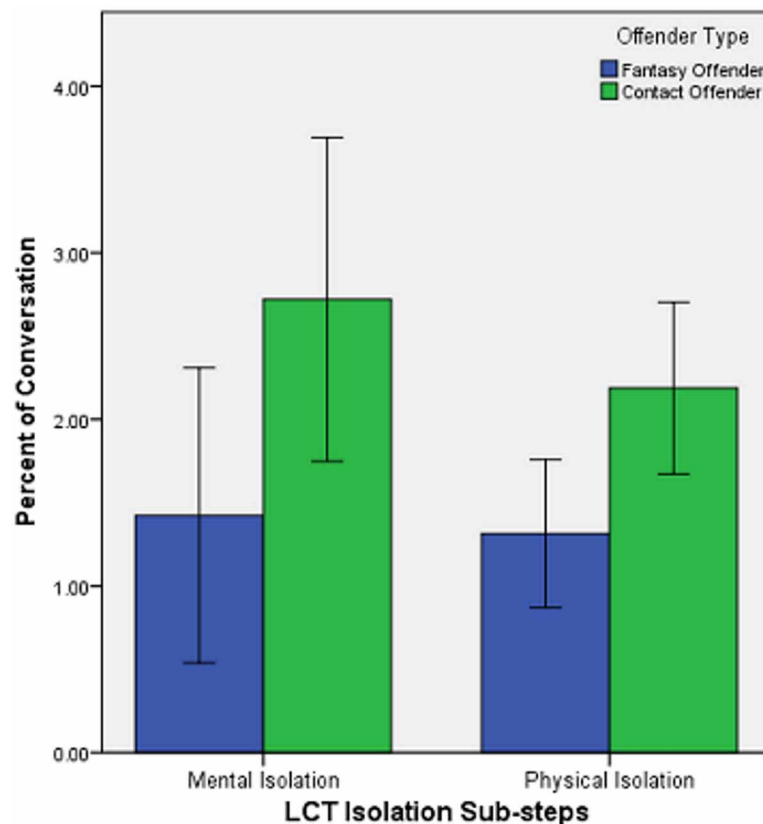
Figure 2. Percentage of the conversation that contact-driven offenders and fantasy-driven offenders spent in each of the two sub-steps of grooming



Approach

Examination of the mean percentage of conversation spent in each of the two Approach sub-steps revealed that the first sub-step of Verbal Lead-Ins (request to meet for sexual activities) was used more often by both Offender Types than the second sub-step of Physical Contact. However, contact-driven offenders used both of the sub-steps of Approach more often than fantasy-driven offenders. The 2 (Offender Type) X 2 (Sub-steps) ANOVA applied to these data revealed that both the main effects of Offender Type, $F(1,71) = 102.07, p < .001, r = 0.77$, and Sub-steps, $F(1,71) = 208.17, p < .001, r = 0.86$, were significant, as was the interaction between Offender Type and Sub-steps, $F(1,71) = 98.45, p < .001, r = 0.76$. The interaction occurred because the difference between contact-driven and fantasy-driven offenders was much larger for the use of Verbal Lead-Ins than for Physical Contact, but follow-up between group tests revealed that both differences were significant, $t(71) = 10.04, p < .001, r = 0.77$ and $t(71) = 5.81, p < .001, r = 0.57$, respectively. Contact-driven offenders used both Verbal Lead-Ins and Physical Contact significantly more than fantasy-driven offenders. Moreover, paired comparisons showed that both offender types used the first sub-step significantly more than the second (fantasy-driven offenders, $t(33) = 4.73, p < .001, r = 0.64$; contact-driven offenders, $t(38) = 14.57, p < .001, r = 0.92$).

Figure 3. Percentage of the conversation that contact-driven offenders and fantasy-driven offenders spent in each of the two sub-steps of isolation



Number and Duration of Chats

To assess the possibility of repeat conversations as well as the total time spent engaging with victims, number of chats sessions and chat durations per victim were determined for each offender type. This information was calculated from information contained within the transcripts, such as timestamps associated with each utterance. Independent sample t-tests were used to compare the total number of chat sessions as well as the total length of the chat conversations for contact- versus fantasy-driven offenders. No significant differences were found for either measure. The mean number of chats per offender was 3.32 while the average total chat length was 204 minutes.

Discussion

In this study, a novel approach was used to analyze communications between pseudo-children and child-sexual offenders using the Luring Communication Theory (Olson et al., 2007) as a basis for differentiating between the contact-driven and fantasy-driven offender types described by Briggs et al. (2011). Our approach revealed both similarities and differences between these two groups of offenders in their use of the LCT main steps and sub-steps as they were engaging in dialog with those that they believed to be children. Given that the LCT contained five main steps, four of which contained additional sub-steps, for ease of exposition our findings across all steps and sub-steps have been summarized in Table 2. The results shown in Table 2 can be viewed in the context of the three predicted outcomes of this study described earlier.

See Table 1 for LCT Step Definition

Prediction 1: Contact-driven offenders, who desire to make offline personal contact, should show more use of Physical Isolation (sub-step of Isolation), Verbal Lead-Ins, and Physical Contact (sub-steps of Approach).

The present results were consistent with the first prediction. When compared to the fantasy-driven offenders, contact-driven offenders were found to spend significantly more of their conversations engaged in the Physical Isolation sub-step of the main Isolation step as well as in both sub-steps of Approach step. The Approach sub-steps included Verbal Lead-Ins and Physical Contact. These findings support the idea that the overall goal of contact-driven offenders was to initiate offline contact, which can be facilitated through the use of Physical Isolation and the sub-steps of Approach. However, it was not anticipated that contact-driven offenders would also use Mental Isolation more than fantasy-driven offenders. Rather, it was expected that this tactic would be employed equally by both offender types as part of their persuasion tactics to maintain contact with the child-victim. But, Olson et al. (2007) noted that both of the sub-steps of Isolation involve distancing the victim from others in their lives, such as guardians, siblings, or peers, thereby increasing victim reliance on the offender. Therefore, it may be easier for a contact-driven offender to draw the victim into a physical encounter if the child does not have strong ties with others and instead places trust in the offender. This result is consistent with the finding of Chiu et al. (2018) that contact offenders are especially concerned about the presence of vigilant guardians and may thus explain why contact-driven offenders tend to engage in more overall Mental as well as Physical Isolation tactics than fantasy-driven offenders.

The present findings with respect to the sub-steps of Approach also are consistent with the different goals of contact- and fantasy-driven offenders as described by Briggs et al. (2011). Contact-driven offenders, who are thought to be focused primarily on initiating an offline relationship, engaged in significantly more Verbal Lead-Ins and Physical Contact strategies than fantasy-driven offenders. Both

Table 2. Summary of findings in main steps and sub-steps

Main Steps	Sub-steps					
<u>Gaining Access</u> <i>Findings:</i> Was least used step (< 3% of total offender communication) No difference between offender types here	<u>No Sub-steps; only main step</u> Gaining access to potential victims					
<u>Development of Deceptive Trust</u> <i>Findings:</i> Second most used main step (~19% of total communication) No difference between offender types here	<u>Activities</u> <i>Findings:</i> 2nd most used sub-step (<4% of total communication) No difference between offender types	<u>Compliments</u> <i>Findings:</i> 3rd most used sub-step (>3% of total communication) No difference between offender types	<u>Personal Information</u> <i>Findings:</i> Most used sub-step (>10% of total communication) No difference between offender types	<u>Relationship Details</u> <i>Findings:</i> 4th most used sub-step (~2% of total communication) No difference between offender types	<u>Gifts</u> <i>Findings:</i> Least used sub-step (<1% total communication) No difference between offender types	
<u>Grooming</u> <i>Findings:</i> Most used main step (>24% of total communications) Fantasy-driven offenders used this step more	<u>Communicative Desensitization</u> <i>Findings:</i> Most used sub-step (20% of total communication) Fantasy-driven offenders used this sub-step more			<u>Reframing</u> <i>Findings:</i> Second most used sub-step (~4% of total communication) No difference between offender types on this sub-step		
<u>Isolation</u> <i>Findings:</i> Second least used main step (~4% of total communication) Contact-driven offenders used this step more	<u>Mental Isolation</u> <i>Findings:</i> Sub-step accounting for approximately 2% of total communication Contact-driven offender used this sub-step more			<u>Physical Isolation</u> <i>Findings:</i> Sub-step accounting for approximately 2% of total communication Contact-driven offenders used this sub-step more		
<u>Approach</u> <i>Findings:</i> Third most used main step (~10% of total communications) Contact-driven offenders used this step more	<u>Verbal Lead Ins</u> <i>Findings:</i> Most used sub-step (~9% of total communication) Contact-driven offenders used this sub-step more			<u>Physical Contact</u> <i>Findings:</i> Second most used sub-step (~1% of total communication) Contact-driven offenders used this sub-step more		
<u>Chat Numbers/Durations</u> <i>Findings:</i> No difference between offender types						

of these sub-steps of Approach likely aid contact-driven offenders in their efforts ultimately to facilitate an in-person meeting with the victim. Since fantasy-driven SOs are only concerned with engaging in online sexual behaviors, they have less reason to engage in these Approach behaviors.

Prediction 2: Fantasy-driven offenders, who desire to maintain an online sexual relationship with the victim, should use more Compliments (sub-step of DDT), Communicative Desensitization, and Reframing (sub-steps of Grooming) than contact-driven offenders.

The findings of this study only partially supported the second prediction. While fantasy-driven SOs were found to use Communicative Desensitization significantly more than contact-driven offenders, these two types of SOs did not differ in their use of Compliments and Reframing. As anticipated, fantasy-driven offenders engaged in significantly more of the Communicative Desensitization sub-step

of Grooming than contact-driven offenders. Since these SOs are presumed to be more concerned with maintaining their online relationship with the victim, it is logical that they would employ Communicative Desensitization. This is a primary tactic by which fantasy offenders increase child receptiveness to sexual content (Lanning, 2010; Olson et al., 2007). Moreover, as Lanning (2010) has noted, Grooming is a *seduction* process that takes time to implement but ultimately facilitates ongoing access to the targeted child, a clear goal of fantasy-driven offenders. In contrast, contact-driven offenders were found in this study to be less likely to prolong the online relationship, consistent with their goals to move on to the steps of Isolation and Approach as quickly as possible in order to secure an in-person meeting with the victim, thus making them less likely to focus on desensitization efforts. In terms of using Compliments and Reframing, while it was thought these strategies might be especially important to the development of an ongoing online relationship for fantasy-driven offenders, in retrospect it makes sense that both types of SOs would make use of both strategies. Compliments help to strengthen relationships with victims, while reframing helps SOs present sexual behavior in a positive light and to normalize the behavior. Both strategies enable SOs to facilitate their deviant interests with victims.

Prediction 3: Fantasy-driven offenders, who are motivated to maintain online contact for as long as possible, would be expected to have a greater number of longer chat sessions than contact-driven offenders, who want to move offline as quickly as possible.

Contrary to this third prediction, it was found that both groups of SOs were similar in the number of chat sessions per victim in which they engaged as well as in the average duration of their chat conversations. Interestingly, neither type of offender dominated the online chats with their victims. Offender utterances accounted for 51% of the conversation while pseudo-children utterances occupied the remaining 49% of the conversation. Given that the presumed goal of fantasy-driven offenders was to cultivate and maintain an online relationship with victims (Briggs et al., 2011), it is not clear why more repeat conversations and/or longer chats did not characterize this offender type in this study, as was found in previous studies (Briggs et al., 2011; Chiu et al., 2018; Dehart et al., 2016). A notable difference between the present study and previous studies using pseudo-children (Briggs et al., 2011; Dehart et al., 2016), however, is the addition of LE pseudo-children. LE pseudo-children may be less likely than PJ vigilante volunteers to take steps to prolong and repeat chat sessions given the focus of LE on prosecutable cases. Also, the present study differed from that of Chiu et al. (2018) who used real children. Future research will be needed to determine the impact of these differences.

SOLUTIONS AND RECOMMENDATIONS

The present results have several important implications for the identification of online SOs. First, the outcomes of this study make a novel contribution to the understanding of the LCT described by Olson et al. (2007), as well as to the classification of offender types proposed by Briggs et al. (2011). This study demonstrates that contact- and fantasy-driven offenders do employ different aspects of luring communication in their online sexual exploitation of victims they believe are children. These outcomes reinforce the utility of the LCT as a general theoretical model for understanding the online communications between the SO and child-victim and underscore the importance of the motivational distinction between offender types proposed by Briggs et al. (2011).

Moreover, these findings expand on earlier work (Kontostathis et al., 2009; McGhee et al., 2011) showing that the LCT steps can be used as a basis for classifying offender versus victim based on chat behavior. While the present study was focused only on offender chats, it does show that the LCT model

is indeed quite relevant to an understanding of SO communications as suggested by Kontostathis et al. (2009) and McGhee et al. (2011). Although Kontostathis et al. (2009) and McGhee et al. (2011) developed coding schemes based on the LCT, they did not differentiate between contact- and fantasy-driven offenders in their populations. Accordingly, their classification accuracy may have been reduced because, as discovered in the present study, the LCT steps are not used equally overall by both offender types. If these researchers had a mixture of offender types in their populations, then variance in the LCT usage attributable to contact- and fantasy-driven offenders may well have influenced their classification accuracy outcomes.

Stemming from previous classification research, a broader implication of the present work is that a much greater predictive power can be achieved in SO classification processes by incorporating knowledge of how the LCT steps are used by these two offender types. The findings of this study strongly suggest that high levels of Communication Desensitization usage likely is indicative of communications from fantasy-driven offenders, whereas high levels of Mental and Physical Isolation, along with Verbal Lead-Ins, likely signifies communications from contact-driven SOs. These types of observations represent a finer-grained diagnostic tool for differentiating offender types, which ultimately may assist in better educating victims and their caregivers about the potential dangers of the Internet. In addition, enhanced predictive power can move the field closer to automating offender identification through the development of software capable of making real-time predictions about the motives of those engaging in sexually explicit chats with children; saving law enforcement agencies time and resources. Most importantly, the results of this study may facilitate efforts to identify online SOs so they can be taken offline and put out of contact with potential victims.

FUTURE RESEARCH DIRECTIONS

Several lines of further research are needed to better understand the present findings and address the limitations of this research. First, although both PJ chats and chats between online SOs and LE officials posing as children were utilized, researchers did not have access to any chats involving online SOs and real children. As such, it is as yet unknown if these results will generalize to online victims other than pseudo-children. Second, the coding scheme used in this research resulted in a large category of offender utterances unrelated to LCT (around 40% of total offender coded lines). As noted above, these utterances represented individual segments of the offenders' conversations that either involved few words, symbols, or abbreviations. In contrast, the LCT codes represented larger individual segments of offender conversations with many more words, symbols, or abbreviations per segment. Thus, in terms of words, the LCT-related codes encompassed about 80% of the offenders' portions of the conversations in the present study. Codes unrelated to the LCT were not parsed carefully in the present study, but should be more closely examined in future work. Third, the Pew Research Center reports that current trends of communication are shifted towards an increased use of SMS messaging and social media on mobile phones versus online instant messaging (Lenhart, 2012). While, it is not clear how this trend would change the nature of SO-victim conversations, this is an issue that needs to be explored in future research. Finally, as noted by many researchers (Aslan, 2011; Kirwan & Power, 2013; Kloess, Beech, & Harkins, 2014; Seto, Wood, Babchishin, & Flynn, 2012), more work is needed to better understand why individuals become online SOs. As this work unfolds, it may inform the process of identifying more specific types of online offenders. Although the present work was guided primarily by the classification of offenders proposed by Briggs et al. (2011), other types of offenders may exist, as suggested by several authors (Aslan, 2011;

Babchishin, Hanson, & VanZuylen, 2015; Kontostathis et al., 2009). If so, it will be important to see how any additional offender types may be similar or different in their use of luring communications.

CONCLUSION

The present study was the first of its kind to investigate the differences between contact- and fantasy-driven offenders using the LCT framework to learn more about their specific motives and behaviors. Clear differences were revealed in how these offender types used luring communications to exploit child victims based on their distinct contact or fantasy motives. Further research in this area is needed, but if this finding proves to be robust, it will provide yet another important way for law enforcement to differentiate these offender types based on samples of their communications with potential victims. However, as noted in several studies (Babchishin et al., 2015; Chiu et al., 2018; Long, Alison, & McManus, 2013; McCarthy, 2010; Merdian et al., 2018), contact- and fantasy-driven SOs may differ in other ways that also will be important to understand, both from the standpoint of identifying these offender types and bringing them to justice. Moreover, as indicated by Hillman, Hooper, and Choo (2014), various significant challenges also will need to be addressed related to the prosecution and remediation of SO's once they are identified and apprehended.

ACKNOWLEDGMENT

The authors wish to thank Nicholas Battis, Natalie Behrens, and the St. Joseph County Prosecutor, Ken Cotter, for their help with project.

REFERENCES

- Aslan, D. (2011). Critically evaluating typologies of internet sex offenders: A psychological perspective. *Journal of Forensic Psychology Practice, 11*(5), 406–431. doi:10.1080/15228932.2011.588925
- Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior, 44*(1), 45–66. doi:10.1007/10508-014-0270-x PMID:24627189
- Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse & Neglect, 44*, 140–149. doi:10.1016/j.chiabu.2014.12.004 PMID:25613089
- Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: Has the internet enabled a new typology of sex offender? *Sexual Abuse, 23*(1), 72–91. doi:10.1177/1079063210384275 PMID:20947699
- Chiu, M. M., Siegfried-Spellar, K., & Ringenberg, T. (2018). Exploring detection of contact vs. fantasy online sexual offenders in chats with minors: Statistical discourse analysis of self-disclosure and emotion words. *Child Abuse & Neglect, 81*, 28–138. doi:10.1016/j.chiabu.2018.04.004 PMID:29730313

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20(1), 37–46. doi:10.1177/001316446002000104

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Davidson, J., & Gottschalk, P. (2011). Characteristics of the Internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies*, 24(1), 23–36. doi:10.1080/1478601X.2011.544188

DeHart, D., Dwyer, G., Seto, M. C., Moran, R., Letourneau, E., & Schwarz-Watts, D. (2016). Internet sexual solicitation of children: A proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression*, 23(1), 77–89. doi:10.1080/13552600.2016.1241309

Dindia, K. (2002). Self-disclosure research: Knowledge through meta-analysis. In M. Allen, R. W. Preiss, B. M. Gayle, & N. A. Burrell (Eds.), *LEA's Communication Series. Interpersonal communication research: Advances through meta-analysis* (pp. 169–185). Mahwah, NJ: Lawrence Erlbaum Associates.

Finkelhor, D., & Araji, S. (1986). Explanations of pedophilia: A four-factor model. *Journal of Sex Research*, 22(2), 145–161. doi:10.1080/00224498609551297

Hall, G. C., & Hirschman, R. (1991). Towards a theory of sexual aggression: A quadripartite model. *Journal of Consulting and Clinical Psychology*, 59(5), 662–669. doi:10.1037/0022-006X.59.5.662 PMID:1955601

Hernandez, A. E. (2000). Self-reported contact sexual offenses by participants in the Federal Bureau of Prisons Sex Offender Treatment Program: Implications for Internet sex offenders. Presented at the 19th Research and Treatment Conference of the Association for the Treatment of Sexual Abusers, San Diego, CA.

Hillman, H., Hooper, C., & Choo, K. K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review*, 30(6), 687–698. doi:10.1016/j.clsr.2014.09.007

Kajzer, M. D., Crowell, C. R., Villano, M., Zenk, J., Segerson, J., Behrens, N., & Battis, N. (2019 in press). Building word-level models from chat dialogue to distinguish sexual offenders from victims and to differentiate among offender types. In R. Johnson (Ed.), *Digital Innovations in Criminal Science Investigations and Forensics*. Hershey, PA: IGI-Global.

Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders*. New York: Cambridge University Press. doi:10.1017/CBO9780511843846

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma, Violence & Abuse*, 15(2), 126–139. doi:10.1177/1524838013511543 PMID:24608540

Kontostathis, A. (2009). ChatCoder: Toward the tracking and categorization of Internet predators. *Proc. Text Mining Workshop 2009 held in conjunction with the Ninth SIAM International Conference on Data Mining (SDM 2009)*.

Kontostathis, A., Edwards, L., Bayzick, J., McGhee, I., Leatherman, A., & Moore, K. (2009). Comparison of rule-based to human analysis of chat logs. In *1st International Workshop on Mining Social Media*. Seville: Bubok.

Lanning, K. (2010). *Child molesters: A behavioral analysis for professionals investigating the sexual exploitation of children*. Alexandria, VA: National Center for Missing & Exploited Children.

Lenhart, A. (2012). *Teens, smartphones & texting*. Pew Research Internet Project. Retrieved from <http://www.pewinternet.org/2012/03/19/teens-smartphones-texting>

Long, M. L., Alison, L. A., & McManus, M. A. (2013). Child pornography and likelihood of contact abuse: A comparison between contact child sexual offenders and noncontact offenders. *Sexual Abuse*, 25(4), 370–395. doi:10.1177/1079063212464398 PMID:23160257

McCarthy, J. A. (2010). Internet sexual activity: A comparison between contact and non-contact child pornography offenders. *Journal of Sexual Aggression*, 16(2), 181–195. doi:10.1080/13552601003760006

McGhee, I., Bayzick, J., Kontostathis, A., Edwards, L., McBride, A., & Jakubowski, E. (2011). Learning to identify Internet sexual predation. *International Journal of Electronic Commerce*, 15(3), 103–122. doi:10.2753/JEC1086-4415150305

McManus, M. A., Almond, L., Cubbon, B., Boulton, L., & Mears, I. (2016). Exploring the online communicative themes of child sex offenders. *Journal of Investigative Psychology and Offender Profiling*, 13(2), 166–179. doi:10.1002/jip.1450

Merdian, H. L., Moghaddam, N., Boer, D. P., Wilson, N., Thakker, J., Curtis, C., & Dawson, D. (2018). Fantasy-driven versus contact-driven users of child sexual exploitation material: Offender classification and implications for their risk assessment. *Sexual Abuse*, 30(3), 230–253. doi:10.1177/1079063216641109 PMID:27052851

Middleton, D., Elliott, I. A., Mandeville-Norden, R., & Beech, A. R. (2006). An investigation into the applicability of the Ward and Siegert Pathways Model of child sexual abuse with Internet offenders. *Psychology, Crime & Law*, 12(6), 589–603. doi:10.1080/10683160600558352

NCMEC. (2018). National center for missing & exploited children. *Cyber Tipline Fact Sheet*. Retrieved from <http://www.missingkids.com/cybertipline/2million>

Olson, L., Daggs, J., Ellevold, B., & Rogers, T. (2007). Entrapping the innocent: Toward a theory of child sexual predators' luring communication. *Communication Theory*, 17(3), 231–251. doi:10.1111/j.1468-2885.2007.00294.x

Pendar, N. (2007). Toward spotting the pedophile. Telling victim from predator in text chats. *International Conference on Semantic Computing (ICSC 2007)*.

Seto, M. C., Wood, J. M., Babchishin, K. M., & Flynn, S. (2012). Online solicitation offenders are different from child pornography offenders and lower risk contact sexual offenders. *Law and Human Behavior*, 36(4), 320–330. doi:10.1037/h0093925 PMID:22849417

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, 7(3), 321–326. doi:10.1089/1094931041291295 PMID:15257832

Ward, T., & Siegert, R. (2002). Toward a comprehensive theory of child sexual abuse: A theory of knitting perspective. *Psychology, Crime & Law*, 8(4), 319–351. doi:10.1080/10683160208401823

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 18(1), 62–70. doi:10.1016/j.avb.2012.09.003

KEY TERMS AND DEFINITIONS

Approach: LCT step used more by contact-driven offenders to facilitate in-person meeting.

Contact-Driven Offender: Online sexual offenders who seek face-to-face contact with their child victims to engage in physical sexual activity (Briggs et al., 2011).

Fantasy-Driven Offender: Online sexual offenders who seek only online interactions with children; often marked by illicit messages, exhibitionism, and child pornography (Briggs et al., 2011).

Grooming: LCT Step used more by fantasy-driven offenders to preparing for sexual behavior.

Isolation: LCT step used more by contact-driven offenders to separate victim from support network.

Perverved Justice: A grass-roots vigilante organization where volunteers pose as children online in order to expose offenders.

Pseudo-Child: A law enforcement officer or a volunteer posing as a child in a chatroom.

ICTs and Sexual Exploitation of Children in Europe

3

László Dornfeld

Ferenc Mádl Institute of Comparative Law, Hungary

INTRODUCTION

‘Child pornography’ is a negative social phenomenon directed against children who are a more vulnerable group of society due to their age, as they are still undergoing intellectual and moral development. It is also a global phenomenon just like cybercrime where the created material can be distributed anywhere in the world.

- With the advance of information technology, new methods of creating, acquiring and distributing child sexual exploitation material have begun to surface. The newest manifestation of this trend is the emergence of the so-called ‘virtual pornography’.
- The technology is relatively cheap, easy to access and portable. It allows for storage of large amounts of material, which would be conspicuous if stored in hard copy.
- Cyberspace provides an inexpensive and anonymous arena for offering, procuring, distributing, transmitting and sharing indecent pictures and videos, and represents an easy and very cheap way to access or obtain child pornography.
- As a result of advances in digital technology and the proliferation of information and communication technologies (ICTs), new forms of crime have emerged, many of which, like “outing and trickery sharing”, “repeated cyberstalking” or “snuff videos”, may overlap with child pornography offenses (Váradi-Csema, 2013, pp. 14-16).

The aim of this chapter is to outline the characteristics of child pornography, including the proper definition of the phenomenon. Then the next chapter discusses how ICTs transformed the production and distribution of child pornographic materials and how modern technology can help in covering the tracks of perpetrators. The chapter also addresses the new phenomenon of ‘virtual child pornography’. The last chapter is about the EU’s response to these criminal behaviors and new developments. The chapter mainly focuses on addressing European answers and regional level supranational legislation. National regulations may appear as examples in the text but not in-depth, taking the limited space of this chapter into consideration.

BACKGROUND

With each technological advance, the availability of child pornography was increasing, the latest being the Internet and ICTs (Quayle, 2011, p. 343). The origins of the development of child pornography can be traced back to the 1960s (Astinova, 2013, p. 4). Throughout these years, there was a gradual relaxation of laws regarding pornography (Gillespie, 2016, p. 227). For example, for almost a decade, all porno-

DOI: 10.4018/978-1-5225-9715-5.ch038

graphic materials were decriminalized in some North European countries, as there was only concern for the consumer and not for the circumstances of the production of these materials. Anti-pornography laws were repelled in 1969 in Denmark and in 1971 in Sweden (Quayle, 2011, p.343). The availability and distribution of child pornography through the Internet has become a social concern for society since the mid-1990s (Akdeniz, 2008, p. 1) The number of prosecutions in the UK involving indecent photographs of children increased from 93 in 1994 to 1,890 in 2003 (Clough, 2010, p. 248).

Sometimes it is questioned whether it is necessary to criminalize child pornography. Astinova argues that it has a preventive function because the demand for such materials provokes further child abuse and exploitation (Astinova, 2013, 4). In Gillespie's opinion, the harm caused to children is the primary reason, while later victimization due to the spread of such material is the secondary reason (Gillespie, 2016, p. 228). The question arises from these opinions: what about those materials which were produced without any victims (digital images, drawings or willing contributors)? This will be addressed later in the chapter.

Child pornography has changed drastically, industrial and technological advances have affected availability, photography, printing and distribution online (Taylor & Quayle, 2003; Aiken, Moran & Berry, 2011). As these materials can be accessed globally through the Internet, an international response is required, especially because of the jurisdictional challenges it raises (Gillespie, 2016, p. 231). In order to fight child pornography, different initiatives were adopted by the international and regional organizations such as the United Nations, the Council of Europe and the European Union (Herczeg, 2014, p. 70).

CHARACTERISTICS OF CHILD PORNOGRAPHY

The following chapters are focusing heavily on the regulations in various international and supranational instruments. Their territorial scopes differ significantly, as one is a global instrument while two were adopted by the Council of Europe (CoE) and thus include countries outside of the Europe Union and one is an EU Directive exclusively for Member States to observe. This means that the confusing situation caused by the already conflicting provisions is much worse.

- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (United Nations General Assembly Resolution A/RES/54/263 of 25 May 2000; 'OPSC')
- Convention on Cybercrime (Council of Europe, ETS No. 185 of 23 November 2001; 'Budapest Convention')
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Council of Europe, CETS No. 201 of 25 October 2007; 'Lanzarote Convention')
- EU Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography ('Directive 2011/93')

The UN's OPSC, an optional protocol to the Convention on the Rights of Child ('CRS'), although drafted in the digital age, pays little attention to the ICT-based abuse of children (Gillespie, 2016, p. 231). The CoE drafted the Budapest Convention as the first international treaty seeking to address Internet and computer crime by harmonizing national laws. As of the end of 2018, more than sixty countries joined the convention ('Council of Europe', 2018) which has a wide range of topics, focusing on both criminal law and criminal procedural law issues. It should not come as a surprise that child sexual exploitation only constitutes a small proportion of the content of the Convention and the only offense it covers is

child pornography (Art. 9). As this was widely criticized, the Lanzarote Convention was adopted by the CoE to tackle all forms of child sexual exploitation (Gillespie, 2016, pp. 231-232).

The European Union had the Framework Decision 2004/68/JHA drafted as part of the ‘third pillar’ to combat child pornography on Union level but it was largely ineffective due to the limitations of EU’s competence in criminal matters. After the Treaty of Lisbon came into effect in 2009, providing a clear mandate to deal with computer crime offenses, the EU has begun to rethink the existing legal regime on both policy and legal level (Buono, 2012, pp. 342-343). As a result of this process, the Directive 2011/93 was drafted, which is legally binding, meaning it is directly enforceable. Thus, it can be considered the “strongest” among the legal instruments.

Terminology

Sexual exploitation of children is a term for a wide range of sexual crimes involving children, like child prostitution or sex tourism. The most important aspect of the term in a digital environment is the creation and distribution of illegal material depicting sexual acts involving children. The proper terminology for describing this phenomenon is much disputed. ‘Child pornography’ is still widely used in legal documents while there is an emerging trend to replace it with other terms, including ‘child sexual abuse material’. The reasoning behind this is that many find the word ‘pornography’ misleading, as it suggests mutual consent, some even going as far as stating that this wording “glorifies” the abusive content (Akdeniz, 2008, p. 11). The Virtual Global Taskforce states that labeling abusive material as ‘pornography’ legitimizes it and distances it from its criminal nature (Mathew, 2009). Some argue that the current terminology “creates a false distinction between the viewing of images and the contact sexual abuse of a child” (“PartnerSPEAK”, 2015).

The European Parliament, in its Resolution on Child Sexual Abuse Online of 11 March 2015, stated that in the future ‘child sexual abuse material’ should be adopted as the correct terminology (2015/2564(RSP), Para. 12). The Terminology Guidelines drafted on 28 January 2016 by the Interagency Working Group on Sexual Exploitation of Children (‘Luxembourg Guidelines’) takes the middle ground and concludes that ‘child pornography’ is still used in legal documents but should be avoided outside of legal context (Greijer & Doek, 2016, p. 38).

This reasoning however is a bit too academic in nature as end material is tied so close to the act of abusing children that it is hard to believe society would become more accepting of the phenomenon just because of the terminology. Yes, some individuals or advocacy groups (like the infamous North American Man/Boy Lovers Association) might try to use it as a justification. There are also people who think positively of online piracy as they see it as a form of freedom from big corporations and there are even Pirate Parties in some national legislations but they rarely advocate for actual Somali pirates. A closer example would be the emergence of the term ‘revenge porn’, the disclosure of private sexual photographs or films, which also constitutes a criminal offense and so far, no one labeled it problematic or glorifying.

Moreover, the proposed replacement terms can also be misleading. For example, ‘abuse’ implicates that children must be harmed while making these materials, which is simply not true given recent developments, like virtual child pornography. In addition, it fails to take into consideration the increasing trend of children willingly producing these materials (Gillespie, 2012, pp. 3-4), as sexually active teenagers with a profound knowledge of ICTs are more likely to do so. This topic will be further explained in a later subtitle of the chapter. Although better solutions, as ‘child exploitative material’ can be coined (Gillespie, 2012, p. 4), the widely used ‘child pornography’ is still the most accurate term, so it will be used throughout the chapter.

Definition of Child Pornography

There are numerous different definitions of the notion in various international, supranational and national legal documents. The scope of differences varies from the use of proper terms to the materials included and methods of committing the crime. Three different factors must be taken into consideration when determining which materials can be considered child pornography. These are:

- Age of the person
- Type of the material
- Nature of the material

The first criterion refers to the person involved in the explicit material, more simply the age requirement to be considered a 'child'. The UN's CRS clearly states that all persons under the age of eighteen shall be protected (Art. 1), which provision also applies to its optional protocol, the OPSC. The CoE's Lanzarote Convention and Budapest Convention also extend protection to anyone under the age of eighteen but the latter also gives the opportunity for signatories to lower the age-limit to sixteen (Art. 9 para. 3). Lastly, the Directive 2011/93 defines 'child' as any person below the age of 18 years. On a policy-making level, this solution is the easiest to implement as people above this age are considered adults capable of consenting to be depicted in pornographic material. Deciding based on physical appearance (bodily developments associated with puberty) and psychological aspects could be a problematic task for law enforcement, as only a few victims are identified even today despite the great effort on the authorities' part, so deciding based on age can be considered the most appropriate method (Gillespie, 2016, pp. 233-235). Although there may be minors psychologically mature enough to give consent and fully understand the consequences of being filmed, ultimately only the person who creates the material will be in the position to know the circumstances of the production (Gillespie, 2010, p. 205).

The biggest problem of age-based approach is the difference in age requirement between having consensual sexual intercourse and recording the act – even between spouses as the marriageable age is lower than 18 in some Member States. The age of consent differs from country to country: in Spain, it is 13 years, 14 years in Hungary (12 if both parties are minors), 15 years in the Czech Republic and 16 years in Belgium (Astinova, 2013, p. 11). The main reasoning behind this is the different consequences of having consensual sex and recording it, as the latter can be harmful to society and can boost the child pornography market (Clough, 2010, p. 257). In addition, it can be harmful for the individual too, as the recording can be posted on the Internet which later can yield search results when, for example, an employer is considering hiring the person. It can be argued that a sixteen-year-old is not ready to make such a decision and it was constantly done so by NGOs (Gillespie, 2012).

The second criterion concerns the type of material. Although we often associate pornography with visually depicting sexual acts, apparently there are other forms of it, like written texts and audio depictions. The international OPSC's scale is the widest as it states 'any representation, by whatever means' although most countries never criminalized all forms (Gillespie, 2016, p. 235). The other three instruments only consider the visual depictions of child sexual exploitation as child pornography. It is a logical choice if the justification for criminalization is based on the harm caused to children as it may cause secondary victimization through the later circulation of images (Taylor-Quayle, 2003, p. 194). Child pornography is not restricted to visual depiction but also can include text and audio depictions. Audio depictions can be just as harmful to children as images as these can be a recording of the sexual abuse of real children. Although it is not a common form of child pornography material, offenders may still find it sexually

arousing (Gillespie, 2010, p. 214). Text-based material is the most problematic since if it does not include identifiable children it is much more in the ‘fantasy’ realm. The fact that these may have artistic value must be also considered, for example, Vladimir Nabokov’s universally acclaimed novel *Lolita*.

Lastly, the nature of the material is to be addressed. There is a wide range of material from pictures that seem harmless in other contexts (e.g. catalog pictures of minors) to hardcore pornography. The UN Special Rapporteur in his report made a distinction between ‘hardcore’, ‘softcore’ and ‘erotic’ material. (Petit, 2004, p. 7-8) However, not all images will be subject to criminal law and thus there is a different categorization:

- Indicative: clothed children, implying a sexual interest in them,
- Indecent: naked children, implying a sexual interest in them,
- Obscene: children in explicit sexual acts.

Traditionally only the obscene images were punishable by criminal law (Gillespie, 2010, p. 206). In 2002, the University College Cork created the COPINE scale, which is a ten-point scale and it is used to categorize the level of seriousness of material with the aim to facilitate law enforcement cooperation (Astinova, 2013, p. 7). Three of the four international instruments (OPSC, Lanzarote Convention, Directive 2011/93) define the nature of the material as “a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes” while the Budapest Convention only contains the child engaging in sexually explicit conduct. The biggest problem with ‘child erotica’ (e.g. sexualized images of children in which the genitalia is covered) is that these can be freely disseminated and can undermine the effort to combat the sexual exploitation of children as a cover-up (Greijer & Doek, 2016, p. 42).

ICTS AND THE CHANGING PATTERNS OF CHILD PORNOGRAPHY

The use of ICTs changes the existing methods of creating and distributing child pornography. The ability to produce child pornography is greatly enhanced as digital images can be produced relatively cheaply without the need for external processing and reproduced with no diminution of quality. Cyberspace offers the opportunity to distribute the materials in large volumes, with minimal cost and relative anonymity (Clough, 2010, p. 249).

Virtual Child Pornography

As the production, possession, and distribution of child pornography is a serious offense in most countries, the perpetrators always try out new ways so that their activity falls into a gray zone of legality, which lowers the likeliness of persecution. It is much easier now, as technology has advanced to the point where a realistic depiction of a child can be created without a real child being involved (Gillespie, 2010, p. 211). The term ‘virtual child pornography’ in a wider sense refers to child pornography in cyberspace (including those with real children involved) while in a narrower, and more commonly used, sense it is pornography directly linked to cyberspace as it can only be produced in cyberspace (Poborilova, 2011, p. 242). There are three principal ways of creating virtual child pornography: 1) manipulating existing images (pseudo-photography) 2) computer-generating new images 3) dressing up adults as if they were minors (Gillespie, 2010, pp. 211-212).

Some authors use ‘pseudo-photography’ and virtual child pornography interchangeably (Gillespie, 2016, p. 245) but the latter term is wider and can include other forms of media like cartoons, manga, anime, etc. Pseudo-photography is created by digitally altering images, ‘blending’ or ‘morphing’ several together, for example putting a children’s face on an adult’s body to make it appear as if it is a child who is engaged in sexual activities (Greijer & Doek, 2016, p.41).

The main distinction Gillespie makes is that some images are only computer-manipulated while others are computer-created. Manipulating images can result in a new photograph that never actually took place (Gillespie, 2016, 245-246). Now even videos can be easily manipulated by the use of Deepfake, a technique for human image synthesis based on artificial intelligence, creating false images in only a few hours (Harris, 2019, p. 100). This can be utilized to produce child pornography and can be considered virtual child pornography. Computer-created images are fully generated by a computer and are not derivatives of photographs. It also must be noted that despite the rapid development of technology it appears that for the foreseeable future child pornography is likely to be created using real children (Clough, 2010, p. 272).

The main principle of virtual child pornography is that there is no abuse or other exploitation of a real child. As there are no children harmed during the production of these materials, the justification for criminalization must be on a different basis (Poborilova, 2011, p. 245). There are voices that claim private thoughts of an individual are part of the freedom of speech and criminalizing it would harm this principle (Gillespie, 2010, p. 213). The UK has put forward three principal justifications for criminalizing virtual child pornography: 1) it reinforces negative views toward children 2) it can be used for grooming children 3) it is frequently found alongside traditional child pornography. These justifications are rather weak: feeling in itself is rarely enough to justify criminalization (as freedom of speech extends to unpopular or offending opinions as well), many activities can benefit grooming unwillingly (more about that in the relevant chapter) and finally there are many things commonly found together with traditional child pornography (Gillespie, 2016, pp. 247-248). The US Supreme Court in the *Ashcroft v. Free Speech Coalition* concluded that prohibiting depictions of child pornography violated the First Amendment of the Constitution. The European Court of Human Rights in the case of *Karttunen v. Finland* in 2011 came to a different conclusion, stating that artists exercising freedom of expression are also subject to duties and responsibilities.

None of the international instruments contains a clear consensus in addressing the dilemma. The OPSC only refers to “child” and nothing indicates that this means anything other than a real child. The Budapest Convention’s scope also extends to “a person appearing to be a minor engaged in sexually explicit conduct” and “realistic images representing a minor engaged in sexually explicit conduct” (Art 9. Para. 2). The Lanzarote Convention contains the definition of “any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes” (Art. 20. Para 2). This means that the two CoE instruments both persecute virtual child pornography but there is an ‘opt-out’ option for all signatory states. The EU Directive 2011/93 clearly covers all type of material and is legally binding for all EU member states.

Self-Generated Content, Sexting, and Sextortion

Another important problem that must be addressed is the question of self-generated content or self-exploitation. This phenomenon stems from increased access and exposure to pornography and the increased sexualization of children in the media (Leary, 2008, p. 18). It means that minors create images depicting themselves naked or during sexual acts and then send these to others. With the rise of the use of mod-

ern ICTs among minors (including computers with built-in web cameras and smartphones with quality cameras), it is becoming more common that they create and forward these materials among themselves.

This activity is often called “sexting” (Merriam-Webster, 2012) and there are even applications which encourage this behavior, like Snapchat. Adults can also engage in sexting between each other so in itself it is not a behavior that can be prohibited. According to research conducted in 2011, 1/3 of European children between the ages of 14-18 have had contact with sexting (Atabekova & Filippov, 2018, p. 765). 70% of 18-19 year-olds surveyed in one study felt pressure from another party to participate in sexting (Váradi-Csema, 2016, p. 642).

It can be as harmful as any other form of sexual exploitation for children. For example, in Denmark, there was a case where a sex video depicting a couple of 15-year-olds was shared by numerous people (mostly students) on the internet, a thousand of whom now face charges (Sorensen, 2018). Europol warns that such material, even if initially shared with innocent intent, often finds its way to “collectors”, who often proceed to exploit the victim, in particular by means of extortion (Europol, 2018).

The law does not specify that child pornography must be created by others to be punishable which means that self-generated content is no exception from the law. Online predators can use it to blackmail children after they send them their first pictures and the scared minor is likely to continue sending more. This behavior is often called “sextortion”. Addressing the problem, the CoE’s Lanzarote Committee released their opinion in July 2019 (Lanzarote Committee, 2019). In their opinion, sexting by children should not be considered child pornography, when it is intended solely for their private use. And children coerced into such conduct should be addressed to victim support and not subjected to criminal prosecution.

Grooming

Grooming can be described as an act befriending minors and then inviting, inducing or coercing them into participating in or observing sexual acts and producing child pornography. Cyberspace facilitates this process in a way that communications can become intimate at a rapid speed (Clough, 2010, p. 332). Research shows that grooming is becoming less frequent as it requires a lot of time and effort to gain the trust of the victim. Now the period between initial engagement with a child and an offending outcome often can be extremely short (Greijer & Doek, 2016, p. 51).

According to a 2014 EU Survey, 20% of 14-16 years old children received sexual images online; 43% had contact online with someone they have not met face to face before, 11% sent their photo or video to these persons, and 14% met online contact offline (Atabekova & Filippov, 2018, p. 765). The Lanzarote Committee adopted an Opinion on the solicitation of children for sexual purposes through information and communication technologies (grooming) in 2015 (Lanzarote Committee, 2015). In this, it is stated that “the solicitation of children through information and communication technologies does not necessarily result in a meeting in person” (Art. 17). This means that grooming that only takes place in online space and does not include offline meetings can be as harmful as any other forms of grooming. Sexual offenses can be perpetrated online which leads to the production of child pornography.

Images of children engaged in sexual activity can be used as tools of grooming children for child pornography and sexual activity (Akdeniz, 2008, 22) and generated material, like the previously mentioned Deepfake videos can be used to encourage children to engage in sexual activity (Harris, 2019, p. 106). Seeing these, children might feel ‘left out’ and may be persuaded to participate actively in sexual activities (Váradi-Csema, 2016, p. 642).

According to O'Brien, there is a cycle of child pornography which first involves showing sexual material to a minor who is then convinced to participate in sexual acts which are filmed at a later stage, creating new material to attract other victims (Akdeniz, 2008, p. 5).

New Means of Distribution

The Budapest Convention requires parties to criminalize the distribution or transmission of child pornography through a computer system (Art. 9. (1)(c)). Although physical distribution was criminalized before the Convention, the increasing use of ICTs required this specification (Clough, 2010, p. 292). It is hard to decide what 'distribution' exactly means as it is undefined in international instruments or national legislations.

In 2006, it was estimated that there were more than 100,000 websites offering child pornography (Clough, 2010, p. 250). However, most of them are not on the surface web, which is well monitored. Dark Web plays a big role in distribution, which is accessible only through specialized applications, such as TOR (The Onion Router), where many criminal groups have been organized around the exchange and trade of child pornography content. Europol confirmed this in 2014, stating that the Darknets and other environments offering a high degree of anonymity are increasingly popular, especially among those with greater security awareness and IT knowledge. Such platforms host hidden services and marketplaces and are increasingly used by child sex offenders and producers (Jeney, 2015, p. 40). For example, the Lolita City community, the 1,500 members of which were eventually exposed by members of the Anonymous hacker group. The US-based pedophile group Candyman had about seven thousand members (Dornfeld & Mezei, 2017, p. 34).

The use of new technologies for distributing child pornography is becoming more regular. Two examples are peer-to-peer (P2P) or file-sharing networks and online streaming services. According to Europol, p2p networks are the main platform to access child abuse material and the principal means for non-commercial distribution. Meanwhile, online streaming means the profit-driven abuse of children overseas, the victims of which live in front of a camera at the request of Westerners (Europol, 2018).

The biggest problem in tackling streaming of material is that it is not covered in most of the international instruments as it is neither "acquisition" or "possession" of the illicit material. The Lanzarote Convention however criminalizes causing or coercing children to participate in child pornographic performances (Art. 21 (a)-(b)). However, it is only on the side of the perpetrator and as they are mostly located outside of Europe, often in Asia and Africa, therefore it is hard to prosecute them for these acts. Art. 24 criminalizes aiding or abetting such actions but it is questionable if simply watching a stream can be taken as such.

Anonymization and Encryption

The notion of anonymity is a very important factor for perpetrators when choosing to utilize the internet and ICTs. Two methods can achieve greater security for them in this regard: anonymization and encryption. While the first one aims at making communication more secure, the latter makes data accessible only to those who have the right encryption key to view it.

Anonymization devices include proxy servers and virtual private networks (VPNs), which allow users to easily obtain an IP address in any other country in the world. Another such tool is the TOR, developed by the United States for military purposes, which protects the content of communications using a hard-to-crack encryption method.

Until a few years ago, the use of steganography (hiding material in another, seemingly harmless file) was significant, but nowadays it is easy to filter out such files. Therefore, encryption programs, the effectiveness of which varies, are more commonly used now (Dornfeld & Mezei, 2016, 35). The nature of encrypted data remains unknown to the investigating authority and cannot be used as evidence. The question, therefore, arises as to whether the defendant may be required to provide the decryption key. In some member states, such as France, there is a provision in the Criminal Code (Art. 434-15-2), stating that the refusal to hand over the password or encryption key to the authorities is a criminal offense, while in Germany, for example, they intend to prevent this by using special police units and raids. In the United States, by contrast, such an obligation was found to be contrary to the prohibition of self-incrimination because the defendant effectively admits having unlawful information in the system.

Although detection is significantly more difficult if the offenders use for example proxy servers, passwords, encryption and/or steganography, according to a US study there are relatively few of them (20%) taking such steps. In addition, it must be noted that the survey was limited to those arrested so it might indicate that more people are actually applying the technology so successfully that they are virtually invisible to law enforcement (Clough, 2010, p. 250).

THE RESPONSE OF THE EUROPEAN UNION AND RECOMMENDATIONS

The European Union is involved in tackling online child pornography and other forms of sexual exploitation of children on many levels: policy, legal framework and institutional. The main legal instrument adopted was the Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography. Art. 3 of the Framework Decision requires the Member States to punish production, distribution, dissemination, transmission, acquisition or possession of child pornography and supplying or making available such material. Art. 8 (3) stated that if a Member State decides not to extradite its own citizen, it has to prosecute when the crime is committed by one of its own nationals outside its territory. Art. 8 (4) instructs Member States to ensure their jurisdiction in cases where the crime was committed by means of a computer system accessed from its territory, whether or not the computer system is in its territory.

In 2007, the European Commission reported that almost all of the Member States had ensured a high level of protection of children from sexual exploitation and abuse but there were problems not addressed by the existing legal regime (Jeney, 2015, p. 13). The Framework Decision proved to be inadequate for requiring proof of “explicit sexual conduct” but not abuse (Astinova, 2013, p. 27). In addition, in the three-pillar system of the EU, the Framework Decision was a rather weak form of secondary legislation, which suffered from many problems. It was similar in nature to Directives but unlike them, it had no direct effect and the transposition was not supervised, causing fragmentation (Dornfeld, 2016, p. 91). The EU’s previous legal regime regarding cybercrime (including online child pornography) was replaced both on a policy and on legislation level following the Treaty of Lisbon’s entry to force in 2009 (Buono, 2012, p. 332).

The first change was on a policy level. In 2009 in Prague at the Conference on ‘Safer Internet for Children - fighting together against illegal content and conduct on-line’ the ‘Prague Declaration’ was adopted. The Declaration is dedicated to the process of improving cooperation between all stakeholders in the field of promoting safer internet and mobile communications, especially for children (Buono, 2012, p. 337). There was a short-lived draft for a new Framework Decision on child pornography in 2009 (Herczeg, 2014, p. 71) but it was soon replaced by a new proposal for a Directive in 2010. This

was adopted in 2011 as the Directive 2011/93, the content of which was addressed before in this chapter on multiple occasions.

The first articles of the Directive are about the definitions, the offenses, aggravating circumstances, etc. There were provisions regarding ICT-based child pornography, like criminalizing pornographic performance (Art. 4(3)), which means forcing a child to participate in pornographic performances (like the streaming mentioned before). Causing and recruiting a child for such performances and attending them was also criminalized. Solicitation for sexual purposes (grooming) is also a new offense in the Directive (Art. 6). Arts 12-13 contain provisions on the liability of legal persons and the relevant sanctions, which are standard regulations in all criminal Directives but here they seem out of place. Although legal persons can also benefit from child pornography (for example trading these materials), there is no precedence of companies engaging in such behavior.

The most interesting provision of the Directive is Art. 25 is titled ‘Measures against websites containing or disseminating child pornography’. It also creates the opportunity for the Member States to create the legal basis for the prompt removal of web pages containing or disseminating child pornography hosted in their territory. If that is not possible, they can order internet service providers to block access to web pages containing or disseminating child pornography for Internet users within their territory. This is often called ‘internet blocking’ and is associated with authoritarian regimes like Russia, Turkey or China. The most serious problem with this solution is that, as it was presented in the chapter, the distribution of child pornography no longer takes place on the surface web. As other areas (like the deep web) is already hidden from the average user, the provision for internet blocking is redundant.

In the proposal of the Directive, the European Commission originally intended to impose a mandatory blocking obligation on the Member States if the effort to remove was unsuccessful. However, during the legislation process, concerns were raised like the potential breach of the right to freedom of expression, lack of adequate legal remedies against blocking measures, the inefficiency of blocking techniques considered easy to circumvent, potential censorship, “overblocking” (i.e. blocking of legal content), etc. So a compromise was reached, making this an optional measure for Member States (Jánoskúti, 2016, p. 74). The biggest fear was that if the states were bound to block the sites containing child pornography it would mean that computer systems and access to websites were to be monitored and confiscation of internet data without authorization could occur (Astinova, 2013, p. 32). In 2016, in total 13 Member States adopted regulation for blocking Internet sites. These are Belgium, Cyprus, France, Greece, Hungary, Italy, Lithuania, Luxembourg, Poland, Portugal, Romania, Spain and Sweden (Jánoskúti, 2016, p. 79). In Hungary, the system is not functioning well, as there were zero sites blocked for child pornography in 2016. Blocking is instead used as a tool to combat illegal online gambling and the selling of fake medicine (Dornfeld & Mezei, 2016, p. 35).

Useful tools for enforcing the provisions of the Directive are the EU’s mutual recognition instruments, which abolish the double criminality requirement with respect to child pornography. Among others, this includes the European Arrest Warrant, the European Investigation Order and the Directive on Confiscation (Jeney, 2015, p. 20). However, these are mostly useful for gathering offline, physical evidence and not e-evidence. Addressing this problem, in 2019 the EU introduced its e-evidence proposal: A Directive and a Regulation. It introduces the “European Preservation Order” and the “European Production Order”. The first one is about preserving data for later confiscation while the latter allows law enforcement to directly request electronic data from any service provider offering services in the EU, irrespective of where the provider’s headquarters are located or where the respective data is stored physically. This is a very big step forward for European legislation.

On a policy level, the EU has adopted the Digital Agenda for Europe as one of the pillars of the Europe 2020 Strategy. As a part of achieving these goals, the European Commission drafted a ‘Strategy for a Better Internet for Children’, which proposed a series of actions to be undertaken by the European Commission, EU Member States and by the ICT industry (Jeney, 2015, p. 23). Victim identification is an important step in tracking down online child pornography, preventing victimization and stopping the further spread of damaging material. Interpol, for example, created an international image database on child sexual exploitation in 2009, providing real-time access to the collected footage, and its February 2016 version provides the ability to analyze video footage (Dornfeld & Mezei, 2017, p. 34). This approach should be strengthened in the EU as well. There is no obligation for the Member States to introduce the registration of sex offenders, as they have the option not to create such a register and there is no European level equivalent either. This means that offenders can easily avoid professional disqualification by cross-border movement, which is unimpaired in the European Union (Jeney, 2015, pp. 42-43).

There were changes in the institutional framework as well. The biggest of those is the establishment of the European Cybercrime Centre (EC3) as a part of Europol. As the Europol has no legal basis to conduct investigations directly, its main goal is to coordinate the work of the Member States’ law enforcement agencies. EC3, in particular, focuses on the fight against online crime that causes serious harm to the victim, including sexual exploitation of children and child pornography. According to a report on the first year of organization, the center was involved in nine large-scale operations against child sexual abuse in 2013 (Dornfeld & Mezei, 2016, 36). Working alongside EC3 is the Joint Cybercrime Action Taskforce (J-CAT), which works on the most important international cybercrime cases, including online sexual exploitation of children that affect the EU Member States and their citizens.

FUTURE RESEARCH DIRECTIONS

There are many topics not addressed in detail in this chapter that are open to future research. One of those is the question of jurisdiction, as the problem of child pornography is a global one, while the legislation response is mainly on a national level. The topic of criminal cooperation is also an interesting one, as there are many cross-border cases and the tools at the disposal of law enforcement are mostly outdated. Legal and investigational responses to the threat of anonymization and encryption is also a hotly debated and interesting topic to research. Victimology and the criminological aspects of increasing youth indecent communication can be potential future areas of research as well.

CONCLUSION

As the chapter shows, online child pornography is a highly complex social phenomenon that targets the most vulnerable in society and recently became an even larger threat due to the rapid development of ICTs. From the start, there are many controversial topics, including the proper term for the phenomenon. One cannot find a settled agreement on the definition, which is not an entirely academic question, as it raises practical issues as well. For example, double criminality is required for law enforcement to request mutual legal assistance from other agencies abroad. There is no unified approach to define child pornography and more harmonization is required on both international and regional level.

The methods of committing the crime are rapidly evolving due to new ICTs. It is hard for legislation and law enforcement to keep up with these new developments. Streaming is currently only punishable

on the creator's side, not the consumer's. File-sharing, deep web groups and other places provide the suitable environment for perpetrators to engage in trading and exchanging these materials. They cover up their tracks and hide evidence using other technologies, such as anonymization and encryption. However, the problem is not entirely technological but also social in nature. Minors use technology to shape their personalities and often engage in indecent communication like sexting, which can be used by predators to coerce them into participating in future child pornographic materials (grooming, sexting). A "cycle" of child pornography can be found.

EU's current legislation, policy and institutional framework is quite effective. However, there are some problems as well, like the utilization of the ineffective tool of internet blocking, the lack of EU-level registration of sex offenders and the lack of engagement in identifying victims. These questions have to be addressed in the future to provide an even better protection on a regional level. The other big problem, however, is much harder to deal with. As online child pornography is a global phenomenon, perpetrators can easily hide outside the EU, like in East and South Asia. A global approach and cooperation is a very important issue for the future.

REFERENCES

- Aiken, M., Moran, M., & Berry, M. J. (2011). *Child abuse material and the Internet: Cyberpsychology of online child related sex offending*. Paper presented at the 29th Meeting of the INTERPOL Specialist Group on Crimes against Children, Lyons, France.
- Akdeniz, Y. (2008). *Internet Child Pornography and the Law National and International Responses*. Ashgate.
- Astinova, M. (2013). *The Crime of Child Pornography: European Legislative and Police Cooperation Initiatives* (Master Thesis). Tilburg University.
- Atabekova, A., & Filippov, V. (2018). Legislation Response to Use of Minors' Self-generated Sexual Content for their ICT-facilitated Sexual Coercion. *European Research Studies Journal*, 21(4), 763–772.
- Buono, L. (2012). Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). *New Journal of European Criminal Law*, 4(3), 332–343. doi:10.1177/203228441200300307
- Clough, J. (2010). *Principles of Cybercrime*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511845123
- Dornfeld, L. (2016). A kiberbűncselekmények nyomozásával kapcsolatban folytatott uniós bünyügyi együttműködés fejlődése. *Külgügyi Szemle*, 15(4), 89–101.
- Dornfeld, L., & Mezei, K. (2017). Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog*, 14(68), 32–37.
- Europol. (2018). *Child sexual exploitation*. Retrieved from: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>
- Gillespie, A. A. (2010). Defining Child Pornography: Challenges for the Law. *Child and Family Law Quarterly*, 22(2), 200–222.

Gillespie, A. A. (2012). *Child pornography: Law and policy*. New York, NY: Routledge. doi:10.4324/9780203818107

Gillespie, A. A. (2016). *Cybercrime: Key issues and debates*. New York, NY: Routledge.

Greijer, S., & Doek, J. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. Luxembourg: ECPAT.

Harris, D. (2019). Deepfakes: False Pornography Is Here and the Law Cannot Protect You. *Duke Law & Technology Review*, 17, 99–128.

Herczeg, J. (2014). Actual problems of possession and viewing child pornography in Internet. *Jura*, 20(1), 70–80.

Jánoskúti, B. (2016). Take down and blocking measures (Art. 25 & recitals 46–47). In *Survey on the transposition of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography*. Retrieved from: <http://missingchildreneurope.eu/Portals/0/Docs/A%20survey%20on%20transposition%20of%20Directive%20against%20child%20sexual%20exploitation%20and%20abuse.pdf>

Jeney, P. (2015). *Combatting child sexual abuse online*. Study for the LIBE Committee. Retrieved from: [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536481/IPOL_STU\(2015\)536481_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536481/IPOL_STU(2015)536481_EN.pdf)

Lanzarote Committee. (2015). *Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Solicitation of children for sexual purposes through information and communication technologies (Grooming)*. Retrieved from: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064de98>

Lanzarote Committee. (2019). *Opinion of the Lanzarote Committee on child sexually suggestive or explicit images and/or videos generated, shared and received by children*. Retrieved from: <https://rm.coe.int/opinion-of-the-lanzarote-committee-on-child-sexually-suggestive-or-exp/168094e72c>

Leary, M. G. (2008). Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation. *Virginia Journal of Social Policy & the Law*, 15(1), 1–50.

Mathew, L. A. (2009). Online Child Safety from Sexual Abuse in India. *Journal of Information Law & Technology*, 1. Retrieved from: https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/mathew

Merriam-Webster. (2008). *Sexting*. Retrieved from: <https://www.merriam-webster.com/dictionary/sexting>

Partner S. P. E. A. K. (2015). *Online child abuse material is not ‘child pornography’*. Retrieved from: <http://www.partnerspeak.org.au/articles/online-child-abuse-material-is-not-pornography>

Petit, J. M. (2004). Rights of the Child: Report submitted by the Special Rapporteur on the sale of children, child prostitution and child pornography. UN Economic and Social Council.

Poborlioiva, M. (2011). Virtual Child Pornography. *Masaryk University Journal of Law and Technology*, 5(2), 241–253.

Quayle, E. (2011). Child pornography. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 343–368). Devon, UK: Willan Publishing.

Sorensen, M. S. (2018). *1,000 Danes Accused of Child Pornography for Sharing Video of Teens*. Retrieved from: <https://www.nytimes.com/2018/01/15/world/europe/denmark-child-pornography-video.html>

Taylor, M., & Quayle, E. (2003). *Child Pornography. An Internet Crime*. Brunner-Routledge.

Váradi-Csema, E. (2013). Gyermekek és fiatalkori bűnözés alapkérdései, különös tekintettel a serdülőkor pszichés sajátosságaira. In Á. Farkas (Ed.), *Tanulmányok a bűnügyi tudományok köréből* (pp. 5–42). Miskolc, Hungary: Gazdász Elasztik.

Váradi-Csema, E. (2016). A gyermek- és fiatalkori kriminalitás. In A. Borbíró, K. Gönczöl, K. Kerecsi, & M. Lévy (Eds.), *Kriminológia* (pp. 616–651). Budapest, Hungary: Wolters Kluwer.

ADDITIONAL READING

Calcara, G. (2013). Role of INTERPOL and Europol in the Fight against Cybercrime, with Particular Reference to the Sexual Exploitation of Children Online and Child Pornography. *Masaryk University Journal of Law and Technology*, 7(1), 19–33.

Chawki, M. (2009). Online Child Sexual Abuse: The French Response. *Journal of Digital Forensics, Security and Law*, 4(4), 7–42.

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Switzerland: Springer. doi:10.1007/978-3-319-15150-2

Döring, N. M. (2012). Internet Sexuality. In Z. Yan (Ed.), *Encyclopedia of Cyber Behavior* (pp. 808–827). IGI Global. doi:10.4018/978-1-4666-0315-8.ch067

Gillespie, A. A. (2012). Jurisdictional issues concerning online child pornography. *International Journal of Law and Information Technology*, 20(3), 151–177. doi:10.1093/ijlit/eas007

McIntyre, T. J. (2010). Blocking Child Pornography on the Internet: European Union Developments. *International Review of Law Computers & Technology*, 24(3), 209–221. doi:10.1080/13600869.2010.522321

Parti, K. (2009). Online child pornography in Hungary - analysis of research findings. *Studia Iuridica Auctoritate Universitatis Pecs Publicata*, 144, 247–265.

KEY TERMS AND DEFINITIONS

3

Anonymization: A process of destroying online tracks of the data that could be used to link it to its originator.

Encryption: The process of encoding a message or information in such a way that only authorized parties can access it.

Grooming: The solicitation of children for sexual purposes.

Internet Blocking: Blocking access for users to certain Internet sites on a national level.

Sexting: A common practice among young persons, which involves taking sexually explicit images of one's self and sending it to others via ICTs.

Sextortion: A form of sexual exploitation during which the victim is coerced to provide sexual favors (including child pornography material) to the perpetrator.

Virtual Child Pornography: Child pornography produced by digitally modifying pre-existing images or fully generated by a computer.

Regulating Misandry: Expanding the Protection Against Online Hate Speech

Maria Mpasdeki

NGO Solidarity Now, Athens, Greece

Zafeiris Tsiftzis

University of Bolton, UK

INTRODUCTION

Internet and social media have become a significant weapon to disseminate and share information around the globe. Yet, the above mentioned are also being misused for hate-crime activities. Hate crimes are criminal offences motivated by prejudice and committed against someone's identity, such as race, national origin, religion and/or other characteristics.

Perpetrators of such crimes are now able to reach a wide audience easily and inexpensively and they are able to carry out such activities in the digital world and commit criminal offences on the basis of prejudice and of certain immutable and innate characteristics of the victim. The so-called hate crimes target groups, such as women and children, disabled people and refugees.

Another type of hate crime can also be consider the online hate speech, or "cyberhate", under specific circumstances. A quite recent research revealed that men - along with women - can also be considered as victims of online hate crimes/cyberhate. More specifically, an Australian survey revealed that 54% of the victims of the reported incident of online abuse were men. The survey also pointed out that men were often subjected to abuse and insults, trolling and malicious gossip and/or rumours.

In the United Kingdom at the same time, the British Law Commission has already decided to review the existing legislation on hate crime. As the 40% of the victims of abuse are men, the Law Commission deliberated to extend the groups of people which could be considered as hate crime victims and be protected by hate crime legislation by including women, men and elderly people.

To that extent, the present contribution focuses on the inefficiencies of the existing legislative measures regarding the online hate speech and demonstrates some good practices. It also gives a general overview of the notion of "misandry" and how it is expressed in the digital world. Finally, it emphasises the need for particular protective measures, not only for women and children, but also for men.

BACKGROUND

Internet has the ability to cross borders, to repeal the existing distances and to set aside the communication barriers (Johnson & Post, 1996, pp. 1347 – 1402). Moreover, internet and social media have become a significant weapon to disseminate and share information around the globe. Still, these digital tools are also being misused for hate-crime activities.

Hate crimes are defined as criminal offences motivated by prejudice and committed against someone's identity, such as race, national origin, religion and/or other characteristics. The perpetrator of a

DOI: 10.4018/978-1-5225-9715-5.ch039

hate crime selects the victim based on its membership of a particular group. In some cases that the crime involves damage to property, and in these cases the property is chosen as well because of its association with a victim group. Furthermore, prejudice or bias could be defined as a preconceived negative opinion, intolerance or hatred directed at a particular group. The group must share a common characteristic that is immutable or fundamental, such as “race”, ethnicity, language, religion, nationality, sexual orientation, or other characteristics (Organisation for Security and Cooperation in Europe, 2014, pp. 21 - 22).

Since internet became very popular, “cyberhate” has emerged as a type of hate speech (Williams, 2006). “Cyberhate” has been manifested as the hateful speech used in an online communication. In particular, cyberhate is connected with social media platforms, such as Facebook and Twitter (Gerstenfeld, 2013; Awan & Zempi, 2016). Unfortunately, there is not a globally accepted current definition of what “cyberhate” consists. For instance, the United States Anti-Defamation League defined cyberhate as “any use of electronic communications technology to spread anti-Semitic, racist, bigoted, extremist or terrorist messages or information. To these, electronic communications technologies belongs the Internet as well as other computer and cell phone-based information technologies” (Anti-Defamation League, 2010). Yet, most of the cyber hate definitions are based on the definition of hate speech or rather hate crime itself.

“Cyberhate crimes” and hate crimes in general target groups, such as women and children, disabled people and refugees. However, a recent study showed that men can also be considered as victims of online hate crimes/cyberhate. The Australian survey demonstrated that 54% of the victims of online abuse were men (Hunt, 2016). The survey also pointed out that men were often subjected to abuse and insults, trolling and malicious gossip and/or rumours.

At the same time, the United Kingdom Law Commission has already decided to review the possibility of extending the already existing legislative protection against hate crime so as to make the current legislation more effective. In fact, the UK Law Commission is examining whether it is necessary to add more features in the protective sphere, such as gender characteristics, age and belonging to a specific subculture (United Kingdom Law Commission, 2018). Since 40% of the victims of abuse are men, the Law Commission deliberated to extend the groups of people which could be considered as hate crimes victims and covered by hate crime legislation by including women, men and elderly people (United Kingdom House of Commons, 2018, p. 9).

The above leads to the following aspects to be examined: First of all, there will be a review of the current international and national legislative framework on regular hate crimes and hate crimes committed in the digital world. Following the review of the existing legislative framework, the present contribution seeks to raise the inefficiencies of the existing legislative measures with regards to the online hate speech and to recognise some good practices. It also reviews the notion of “misandry” and how it is expressed throughout the digital world. Finally, it emphasises the need for particular protective measures, not only for women and children, but also for men.

International and Regional Legal Texts on Hate Crime

Hate crime is grounded in the principles of equal rights and tolerance which are incorporated in several international and regional human rights legal texts. To this end, the national policies and legislative measures towards the prevention of hate speech are developed to fulfil the international standards and to comply with the obligations of States. Therefore, to identify the effectiveness of the online hate speech regulations, it is worth pointing out briefly some of the most important international and regional legal instruments applicable to this matter.

International Legal Materials

International Covenant on Civil and Political Rights (ICCPR)

International Covenant on Civil and Political Rights (ICCPR) of 1966 constitutes the most important – after the Universal Declaration of Human Rights – legal instruments in the field of the protection of human rights. Article 20, para. 2 introduces that “[...] any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law [...]”. This article should be read with the limitation of the freedom of expression set out in article 19, para. 3, of ICCPR. It highlights that some limitations are “[...] necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order or of public health or morals [...]”.

The Human Rights Committee has explained further the difference between the two norms. In General Comment No. 34, the Human Rights Committee argued that “[...] what distinguishes the acts addressed in article 20 from other acts that may also be subject to limitations, is that for the acts addressed in article 20, the Covenant indicates the specific response required from the State: their prohibition by law. It is only to this extent that article 20 may be considered as *lex specialis* with regard to article 19. The acts referred to in article 20, paragraph 2, must cumulatively (a) advocate, (b) be for purposes of national, racial or religious hatred, and, (c) constitute incitement to discrimination, hostility or violence. By “advocacy” is meant public forms of expression that are intended to elicit action or response. By “hatred” is meant intense emotions of opprobrium, enmity and detestation towards a target group “Incitement” refers to the need for the advocacy to be likely to trigger imminent acts of discrimination, hostility or violence. It would be sufficient that the incitement relate to any one of the three outcomes: discrimination, hostility or violence [...]” (United Nations Human Rights Committee, 2011).

The exercise of violence is the main result of the commission of a hate speech crime. This violence aims to diminish the rights and the freedoms of the targeted group by making it an object of discrimination. Moreover, hate speech is also used to stereotype a group by identifying and highlighting one or more of its negative characteristics.

United Nations Convention for the Elimination of Racial Discrimination (CERD)

Apart from ICCPR, the Convention for the Elimination of Racial Discrimination (CERD) also emphasises the obligation of States to respond to extreme manifestations of hate speech. Article 4 of the CERD encourages State Parties to “[...] condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention, *inter alia*:

- (a) Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof;

- (b) Shall declare illegal and prohibit organizations, and also organized and all other propaganda activities, which promote and incite racial discrimination, and shall recognize participation in such organizations or activities as an offence punishable by law;
- (c) Shall not permit public authorities or public institutions, national or local, to promote or incite racial discrimination [...].

Additionally, General Recommendations No. 7 and No. 15 of Committee of CERD reaffirmed the requisite character of this obligation (United Nations Committee on the Elimination of Racial Discrimination, 1985). For instance, General Recommendation n. 15 explains further that States have to monitor that the appropriate legislation is enforced (United Nations Committee on the Elimination of Racial Discrimination, 1993).

Regional Legal Texts

European Convention on Human Rights (ECHR)

Similar provisions can be found in regional human rights instruments. Article 10 of the European Convention on Human Rights (ECHR)¹ states that “ [...] everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers [...]”. Similarly, the European Court of Human Rights (ECtHR) emphasised that the freedom of expression constitutes a fundamental value of democracy and the rule of law. More precisely, the ECtHR advised that the freedom of expression is not only applicable to “ [...] information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb [...]” (European Court of Human Rights, *Handyside v. United Kingdom*, 1976).

Council of Europe Additional Protocol to the Convention on Cybercrime 2003

The Additional Protocol to the Convention on Cybercrime was adopted in 2003 in order to criminalise acts of racist and xenophobic nature committed through computer systems. At the time of its adoption, there was an important need for suppression of racist and xenophobic acts and on the other hand a need for balance the freedom of expression through computer systems. More particularly, it is highlighted that the signatory parties of the Protocol should “(...) adopt such legislative and other measures as may be necessary to establish as criminal offences (...) distributing, or otherwise making available, racist and xenophobic material to the public through a computer system”.

European Union Council Framework Decision 2008/913/JHA on Racism and Xenophobia

The Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law recognises that hatred and violence against persons or a group of persons based on their race, colour, religion, descent or national or ethnic origin constitutes a serious threat and should be criminalised. More specifically, according to the Framework Decision, the public incitement to the abovementioned acts and/or their commission by public dissemination or distribution of pictures and other material have to be punishable².

American Convention on Human Rights (ACHR)

Article 13 of the American Convention on Human Rights (ACHR)³ sets out that “ [...] everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one’s choice [...]”. The above mentioned article includes a more narrow approach of the Article 20 of ICCPR. The text of art. 13 (5) is the following, “Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, colour, religion, language, or national origin shall be considered offenses punishable by law”. In fact, it fails to include “hostility” and “discrimination” among the aims pursued by hate speech and resorts rather vaguely to the expression “any other similar action” (American Convention on Human Rights, Article 13).

African Charter on Human and Peoples’ Rights (ACHPR)

The African Charter on Human and Peoples’ Rights (ACHPR)⁴ highlights that “ [...] 1. every individual shall have the right to receive information. 2. Every individual shall have the right to express and disseminate his opinions within the law [...]” (African Charter on Human and Peoples’ Rights, Article 9).

In other words, all of the international and regional legal instruments prescribe limitations on freedom of speech in cases that the speech is discriminatorily aimed at individuals (Webb, 2011, pp. 446 - 447).

Effectiveness of the Current Regulations on Online Hate Speech

Despite the existing regulations with regards to the protection of individuals by online hate crime violations, there are several recorded violations as shown on the existing national case law. The case law revealed how difficult is for States to comply with the online hate crime regulations. It also acknowledges the different approaches adopted by European States and the United States of America. This resulted in problems within the realm of the jurisdictional and technical implementation of regulatory orders (Alkiviadou, 2017). The main reason for this is the fact that the online world has no frontiers and it is very easy for multiple jurisdictions to be involved in an online hate crime case.

The Fredrick Töben case

In 1999, Fredrick Töben was arrested - while he was visiting Germany - because he had uploaded anti-Semitic material and information onto his website, an action that was violating Germany’s Holocaust Law. The website was registered in Australia. Thus, a court of first instance argued that Germany is not able to control that material of his website. However, the German High Court reversed this decision and pointed out that “German authorities may take legal action against foreigners who upload content that is illegal in Germany – even though the Websites may be located elsewhere” (Van Blarcum, 2005). This example case revealed the broad interpretation given by the German courts to the exercise of jurisdiction for matters with regards to internet.

THE YAHOO! INC. V. LA LIGUE CONTRE LE RACISME ET L'ANTISÉMITISME CASE

The case of *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme et al* was another case that demonstrated the legal and technical consequences of jurisdictional issues regarding internet regulations (*The Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisémitisme*, 2001). In 2001, the League against Racism and Anti-Semitism and the Union of Jewish Students of France issued proceedings against Yahoo! for offering souvenirs of Nazi for auction on its website. Yahoo! recalled the boundaries of the French law jurisdiction as the content was uploaded in the United States of America where the conduct and material was permitted under the First Amendment. Yet, Yahoo!'s argument was not accepted by the court. The French court “applied an effects-based jurisdictional analysis and granted prescriptive jurisdiction describing the sale of Nazi paraphernalia” (Bank, 2010, p. 235). Therefore, the French Court held that Yahoo! was liable for its effects in France under the R. 645-1 of the French Criminal Code (R. 645-1 of the French Criminal Code outlaws the sale, exchange or display of Nazi related materials or Third Reich souvenirs). Moreover, the French court requested from Yahoo! to confirm that French citizens would not have access to the auctions of Nazi objects; Yahoo! was also subjected to 100,000.00 francs for every failure to comply with the order (*The Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisémitisme*, 2001). The order further summarised that Yahoo! should “take all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artifact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes” (*The Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisémitisme*, 2001).

Besides, the French Court commented upon the jurisdictional application of the order by underlining that the main issue in this case was whether it was “consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation” (*The Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisémitisme*, 2001).

The Yahoo! case confirmed again the wide range of technical issues and legal consequences of jurisdictional application with regards to internet regulations. Taking into account the absence of actual and physical borderline of the internet and the use of social media, it is easy not easy enough to control and monitor someone's access to information. For instance, someone has access to a kind of material which is a criminal offence for his country. Like France and United States of America in this case, States meet legal obstacles in case that they decide to set restrictive measures for the material available online. In fact, the notion of the territorial use of internet has a different meaning in the digital and social media era (Bank, 2010, p. 235).

The Warman v Kyburz case

In 2002, the *Warman v Kyburz* case dealt with anti-Semitic content of Kyburz' website. More specifically, a lawyer named Richard Warman turned against Fred Kyburz who was accused of disseminating hateful content for Jewish people, by violating the Canadian Human Rights Act. The Canadian Human Rights Tribunal examined the problems raised with regards to the internet borders (*Warman v Kyburz*, 2003). In particular, the Canadian Human Rights Tribunal argued that, due to the nature of internet “including the jurisdictional challenges arising from the borderless world of cyberspace, as well as the ‘moving targets’ created by the use of mirror sites, raise real concerns as to the efficacy of cease and desist orders in relation to hate messages disseminated on the Internet” (*Warman v Kyburz*, 2003).

FOCUS OF THE ARTICLE

Current Challenges of the Regulation on Online Hate Crime

The above cases reflected some of the major difficulties related to the regulation of the online hate crime activities based on jurisdiction. Yet, the notion of jurisdiction of the internet remains unclear due to its borderless nature (Alkiviadou, 2017). Regional judicial human rights mechanisms, such as the European Court of Human Rights and national courts have interpreted the notion of jurisdiction more broadly. However, the contribution of the judiciary bodies - regional and national - does not stay only on the examination of the jurisdiction and/or anti-Semitic cases.

Nowadays, online hate crime activities have the form of hurtful comments across all social media platforms (trolling), online threats against a person, group of people or organisation, disclosure of private sexual images without consent, online harassment (sexual or psychological), grooming, online stalking and virtual mobbing. Individuals who are considered as victims of those crimes are often people who belong in vulnerable groups, such as women, children, people with disabilities (Fundamental Rights Agency, 2015), LGBTQI, immigrants and refugees. The so-called “cyberhate” does not have a standard definition, but all the aforementioned activities (or lack of actions) are included, as forms of it (Asko, 2017).

The UK Home Affairs Committee referenced that women are the main victims of harassment on social media. The most common type of harassment is sending sexist messages. Women who are using twitter have witnessed that they have received abusive messages. At the same time, around a third of women experienced “politically extremist hate messages, unwanted sexual messages or images, stalking, and threats of violence” (United Kingdom House of Commons, 2018, p. 8). This is the main reason that the UK Law Commission started negotiations in order to include misogyny as a separate hate crime (United Kingdom House of Commons, 2018b).

Moreover, online harassment and cyber hate crime can also affect children. Cyber bullying is defined as bullying (abusive behaviour) that is taking place through digital means, such as electronic devices. Trolling messages and threats, sending, posting, or sharing negative or harmful content about someone else at online fora constitute a form of cyber bullying. Since 2015, in the United Kingdom, 4,541 child line counselling sessions were taken place whereas cyber bullying was mentioned. This was a 13% increase within 2 years' time (United Kingdom House of Commons, 2017).

In the digital era and hidden behind a computer screen, both men and women could be equally considered as victims. A recent Australian research reveals that men are victims of online harassment. A 54% of the victims of online abuse were men (Hunt, 2018). The survey also pointed out that men were often subjected to abuse and insults, trolling and malicious gossip and/or rumours (Hunt, 2018). Simultaneously, in the United States of America almost 20% of the complaints with regards to sexual harassment complaints at work were filed by men. Similarly, a UK survey found that 20% of men had experienced of sexual harassment in the United Kingdom. The same survey also revealed that 79% of male victims kept it to themselves because of the fear of embarrassment in case of raising a complaint and the concern that their complaints will not be taken seriously (Lapin, 2018). In other words, along with misogyny, misandry would constitute a major concern for the modern societies in the online hate crime regulation.

Misandry [deriving from the Greek words *μίσος* (hatred) and *άνήρ* (man)] is defined as “the hatred of men”, “the feeling of hating or strongly disliking men, or being prejudiced against them”. Dr. Paul Nathanson and Dr. Katherine Young note that the term “misandry”, “like misogyny, (...) is culturally propagated hatred”. The UK Law Commission is currently preparing a review project of hate crime legislation. More particularly, it intends to review the range of protected characteristics and the potential

need of including more characteristics under the legislative protection. The crimes motivated by hatred based on gender characteristics (misogyny and misandry) are going to be reviewed on whether they can be classified as hate crimes.

However, the national regulation on the online hate crime should not be ‘gender based’. All individuals should enjoy the same rights and should have equal protection by the law. In case that a State adopts a ‘gender based’ regulation on online hate crimes, it looks that it appoints one gender always as the perpetrator of the online hate crime and the other as the victim. But, if States deviate for the adoption of a ‘gender based’ approach towards their national policies, this will fail to address misogyny as the main issue. It will also lead to reporting misandry online hate crime incidents. Besides, seventy years after the adoption of the Universal Declaration of Human Rights, domestic regulations that provides with special protection to women seem to be anachronistic, whilst Article 20 of the EU Charter confirms that everyone is equal before the law.

The issue of online hate is moving in new dimensions. Perpetrators of online hate speech find an array of possibilities to use and abuse the internet for purposes of victimisation. On the other hand, victims - both women and men - have been exposed to dangers due to the misuse of the social media platforms. Quite recently, more than 1,300 cases of sextortion were reported to the UK National Crime Agency and the UK Anti-Kidnap and Extortion Unit (AKEU) by the police across the UK. According to this, organised groups are using fake profiles on social media and/or dating websites in order to befriend victims - mostly young males aged 17-25 - and encourage them to livestream sexual activities which are recorded and then they threaten them to share with the victim’s friends and family unless they are paid. At least five British men and boys have killed themselves after being targeted of sextortion (Dearden, 2018).

SOLUTION AND RECOMMENDATION

The above reveals that victims of the online hate crime are not only women.

The need to enact proper legislative measures to promote the safe use of internet and social media is more than necessary. Unfortunately, even if the internet’s capacity is to promote the communication around the globe, in some cases internet is used by some people - individual and/groups - to transmit anti-Muslim and anti-Semitism ideologies, racism and xenophobia feelings, homophobia, misogyny and misandry and other forms of hate. This type of hate can be found on several websites and blogs, as well as in chat rooms and social media.

States lately have adopted national action plans on how to respond to online hate crimes. In some countries as the United Kingdom, the online hate crime is treated the same as the face-to-face hate crime. However, the real challenge on this matter is how to tackle online hate crime efficiently and follow the rapid development of technology.

The emergence of the online world and social media platforms has increased the practice of self-regulation. Self-regulation is the technique of a social media platform to develop its own policy and use regulatory tools for its users; nowadays, it is considered as the most preferred approach for combating online hate speech, although it also needs improvement, as self-regulation itself does not guarantee effectiveness and efficient protection. In order for self-regulatory tools to be effective, it is important to present a strong

On 31 May 2016, the European Commission, together with Facebook, YouTube (Google), Twitter and Microsoft, agreed a ‘code of conduct’ on fighting hate speech. To this end, in 2018, German police officers have the responsibility to undertake a crackdown on racist or xenophobic social postings at a

national level, as a result, they traced the identity and the homes of 36 people suspected of being behind the posts. At the same time, Germany has approved a new bill regarding the punishment of the social networking sites in case that they fail to remove illegal content such as hate speech and/or defamatory fake news. If they fail to do so, the laws impose fines of up to 50 million euros on Facebook, Twitter and other social media platforms.

REFERENCES

ADL. (2010). Responding to Cyber hate. Toolkit for Action. *Anti-Defamation League*. Retrieved from <http://www.adl.org/assets/pdf/combating-hate/ADL-Responding-to-CyberhateToolkit.pdf>

African Charter on Human and Peoples' Rights, adopted June 27, 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 ILM 58, art. 9 (entered into force Oct. 21, 1986).

Alkiviadou N. (2017), Regulating Internet Hate: A Flying Pig? *JIPITEC*.

American Convention on Human Rights American Convention on Human Rights, opened for signature Nov. 22, 1969, 1144 UNTS 123, art. 13 (entered into force July 18, 1978).

Asko, D. (2017). *Cyberhate on cyber space: cyberbullying – A new phenomenon of violence among youth*. Council of Europe.

Awan, I., & Zempi, I. (2016). The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts. *Aggression and Violent Behavior*, 27, 1–8.

Bank, J. (2010), Regulating Hate Speech Online. *International Review of Law, Computers & Technology*, 3, 235.

Collinsdictionary.com. (2018). *Misandry definition and meaning* | *Collins English Dictionary*. Available at: <https://www.collinsdictionary.com/dictionary/english/misandry>

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

Dearden, L. (2018). *Five British men have killed themselves after falling victim to online 'sextortion', police reveal*. Independent.

European Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature Nov. 4, 1950, 213 UNTS 221, art. 10, (entered into force Sept. 3, 1953).

Fundamental Rights Agency, Equal Protection for All Victims of Hate Crime: The Case of People with Disabilities, 03/2015, General Comment n. 34 by the Committee on Human Rights General Recommendation n. 15 of the Committee on the Elimination of Racial Discrimination General Recommendation n. 7 of the Committee on the Elimination of Racial Discrimination.

Gerstenfeld, P. (2013). *Hate Crimes: Causes, Control and Controversies*. Sage Publications.

Guide to the Code of Conduct on Hate Speech - EDRI. (2018). Retrieved from <https://edri.org/guide-code-conduct-hate-speech/>

Handyside v. United Kingdom, 24 Eur. Ct. HR (set. A) at 23. (1976). Retrieved from http://www.coe.int/en/web/octopus/blog/-/blogs/cyberhate-on-cyber-space-cyberbullying-a-new-phenomenon-of-violence-among-youth#_ftnref1

Hunt, E. (2017). *Higher proportion of men than women report online abuse in survey*. Retrieved from <https://www.theguardian.com/media/2016/sep/06/higher-proportion-of-men-than-women-report-online-abuse-in-survey>

Johnson, D., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, 48(5), 1367. doi:10.2307/1229390

Lapin, T. (2018). *The surprising number of men who complain of workplace sexual harassment*. Available at <https://nypost.com/2018/04/09/the-surprising-number-of-men-who-complain-of-workplace-sexual-harassment/>

Lawcom.gov.uk. (2018). *Hate Crime | Law Commission*. Available at: <https://www.lawcom.gov.uk/project/hate-crime/>

Macmillandictionary.com. (2018). *misandry (noun) definition and synonyms | Macmillan Dictionary*. Available at: <https://www.macmillandictionary.com/dictionary/british/misandry>

Online hate crime to be treated the same as face-to-face crime in the UK. (2018). Retrieved from <https://techcrunch.com/2017/08/21/online-hate-crime-to-be-treated-the-same-as-face-to-face-crime-in-the-uk/?guccounter=1>

Prosecuting Hate Crimes. A Practical Guide | OSCE. (2018). Retrieved from <https://www.osce.org/odihr/prosecutorsguide>

Toben, Gerald Frederick v State of Victoria & Allen, Graham, No. CCA 10 of 1989 (Supreme Court of Victoria, Appeal Division 1990).

UK House of Commons. (2017). *Online harassment and cyberbullying by Pat Strickland and Jack Dent, Number 07967*. Author.

UK House of Commons. (2018). *Misogyny as a Hate Crime, Number CDP-2018-0057*. Author.

UK House of Commons Library. (2018). *Misogyny as a hate crime, A Westminster Hall debate on Misogyny as a hate crime is scheduled for Wednesday 7 March 2018 at 9.30am. The Member leading the debate is Melanie Onn MP*. Available at <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CDP-2018-0057>

Van Blarcum, C. D. (2005). Internet Hate Speech: The European Framework and the Merging American Haven. *Washington and Lee Law Review*, 2, 804.

Warman v Kyburz, (2003 CHRT 18) (2003/05/09) para. 81.

Webb, T. J. (2011), Verbal Poison-Criminating Hate Speech: A Comparative Analyse and a Proposal for the American System. *Washburn L.J.*, 50.

Williams, M. (2006). *Virtually Criminal: Crime, Deviance and Regulation Online*. Routledge.

Yahoo, Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme, et al 145 F. Supp. 2d 1168, Case No. C-00-21275JF (N.D. Ca., September 24, 2001).

ENDNOTES

- ¹ European Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature Nov. 4, 1950, 213 UNTS 221, art. 10, (entered into force Sept. 3, 1953).
- ² Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.
- ³ American Convention on Human Rights, opened for signature Nov. 22, 1969, 1144 UNTS 123, art. 13 (entered into force July 18, 1978).
- ⁴ African Charter on Human and Peoples' Rights, adopted June 27, 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 ILM 58, art. 9 (entered into force Oct. 21, 1986).

Online Hate Crimes Against Women (CYBER VAWG)

3

Tehmina Khan

RMIT University, Australia

INTRODUCTION

Misogyny takes numerous forms in the context of social systems and organisations. Manne (2018) describes it as a serious issue that results from discomfort and hostility when a well-entrenched system of social norms is challenged. Women who challenge gendered norms or expectations, who disrupt or pose a threat to gendered social hierarchies or powerful women who do not yield their power in service of men's interests face misogyny (ibid.) or cyber violence (cyber VAWG). The key objective in this article is to provide a detailed meaning and consideration of cyber VAWG with numerous real-life examples provided in literature and to analyse its potential impacts. A literature review of academic and non-academic articles has been undertaken to identify the meaning of cyber VAWG, its impacts and recommendations to tackle cyber VAWG.

BACKGROUND

The increasing availability of internet and access to social media by the masses has resulted in the increasing occurrences of cyber violence against women and girls (cyber VAWG). The term cyber VAWG encompasses multiple forms of exhibitions of violence against females in the online environment ranging from hostility to threats, exploitation and sexual harassment. Cyber VAWG is an additional layer of misogynistic practices, undertaken in the online environment. Manne (2018) has critically described misogyny as a branch of a patriarchal order with the objective of exercising control, power and subjugation, while maintaining the governing ideology of hostility against females. Gender imbalance, gender inequality and gender segregation in the real world, in organisations and professions impact the content which is produced, commercialised and disseminated; misogynistic behaviours are now rapidly increasing online (Swaminathan, 2014).

According to Ging and Siapara (2018) certain types of females have become key targets for online shaming, or “digital pillory.” Hess and Waller (2014) have identified these females as social justice warriors (SJW), the “slut” (as labelled by misogynists)- women in tech and gaming who have dared to challenge entrenched norms of the IT industry which is still male dominated, or any woman who is perceived as publicly questioning or disrupting gendered power relations. The “slut” is a derogatory term used for a woman who promotes any aspect of feminism or women's rights in the online medium.

The disciplining function of online discourses against these women as Alvares (2018) has identified, becomes a means of violent reinforcement of gendered power relations through online misogyny. Cole (2015) has captured the experiences of women who publicly promote women's rights or any aspect related to feminism through the following quotes: Christina (2012), a blogger “get[s] this all the time. I get this so often, I've lost track. As has every other woman I know who speaks publicly about feminism.”

DOI: 10.4018/978-1-5225-9715-5.ch040

Journalist and blogger Jessica Valenti (2014) has been quoted by Cole (2015) about projecting her views on Facebook: “I spen[t] the better part of the day fielding tweets and messages about what a slut I am. That I should be ‘jizzed on’ ... that I want to be gangbanged, that I’m worthless.” As identified by Cole (2015) and in various other published works on misogyny through social media, rape is the most frequently used threat in response to women online (Stanton, 2011). The threat of rape in a large portion of tweets is often accompanied by an emoticon or an acronym such as “LOL,” or a joke; humor is used in order to make the violence socially acceptable and remains as a part of the disciplining process (Cole, 2015). Doyle (2011) re-emphasizes the gendered nature of violent discourse committed online as “What matters is not which guys said it: What matters is that, when you put their statements side-by-side, they all sound like *the exact same guy*. And when you look at what they’re saying, how similar these slurs and insults and threats we get actually are, they always sound like they’re speaking to *the exact same woman*. When men are using the same insults and sentiments to shut down women ... we know that it’s not about us; it’s about gender”. Regardless of which legislation is looked at, threat to commit rape is considered a sexual offence. Rape threats are not the only forms of cyber VAWG undertaken in the online environment. There are numerous other types of cyber VAWG. The objective of this Chapter is to consider cyber VAWG in detail based on a review of prior academic and non-academic literature. Numerous real-life examples of cyber VAWG and cyber misogyny are provided to highlight types of cyber VAWG and the extremely negative impacts of VAWG crimes.

METHODOLOGY

Searches were undertaken in Google Scholar and Google using search terms such as Cyber violence against women and girls, ‘cyber bullying’, ‘cyber violence’, ‘cyber violence against women and girls’, ‘online harassment’, and iterations thereof between October and November 2018. Multiple government reports and media coverage as well as academic literature on the topic of cyber VAWG were identified. These have been cited. The approach adopted in this article has been a review of academic and non-academic literature on cyber VAWG.

Cyber Misogyny/VAWG Hate Crimes

Gender violence has been defined by the UN Committee on the Elimination of Discrimination against Women (CEDAW), general Recommendation 19 as “violence that is directed against a woman because she is a woman that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty (CEDAW, 1992). CEDAW’s general recommendation 35 extends gender-based violence against women to multiple forms including in technology mediated settings and redefines gender based violence through technology mediated environments occurring in internet and digital spaces as cyber VAWG (CEDAW, 2017).

There are numerous terms which are used to describe online hate crimes specifically targeted against women including: gendered cyber hate, technology-facilitated violence, tech-related violence, online abuse, hate speech online, digital violence, networked harassment, cyber bullying, cyber harassment, online violence against women (VaW), and online misogyny (Ging and Siapera, 2018). References to these multiple terms as used in literature are used to capture the forms of gendered online abuse, the impacts of the abuse, implications as well as recommendations to mitigate the issue. Technology related human rights violations are defined in UN General Assembly’s (2013) Consensus Resolution as “

information-technology-related violations, abuses and violence against women, including women human rights defenders, such as online harassment, cyber stalking, violation of privacy, censorship and hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or to incite other violations and abuses against them...” (UNGA, 2014).

For cyber VAWG to occur, the main condition which needs to be met is the availability of Internet. Fifty-six per cent of the world population has access to the Internet and in most countries male access to the Internet is more than female access except in the Americas where it is roughly equal. A social networking platform has been found to act as the most popular medium for cyber VAWG (Ottawa Coalition to End Violence Against Women, 2016). The internet and its various platforms are now acting as a medium to promote toxic masculinity and as a result cyber-misogyny.

Cyber misogyny hate crimes are prevalent and increasing in societies and cyber VAWG has been declared as being of pandemic proportion with limited accountabilities enforced against perpetrators (UN Broadband Commission for Digital Development Working Group on Broadband and Gender, 2015). Anonymity is a key feature of online engagement and according to Zimmerman (2016) deindividuation which encourages people to exhibit violent, disinhibited behaviour, loss of control and personal constraint turns into “cyber dis-inhibition that occurs mainly because of the anonymous nature of the internet. Individuals may behave in ways that contradict normative behaviour when they do not identify with a particular online community and are free to leave without desire to return (...) individuals are able to freely make any statements, act in any online behaviour available, or even be whoever they want to be, only to simply log off at the end of the day. This ability to disconnect might trump the need for permission to behave in certain ways”. There are additional factors which have resulted in increasing cyber VAWG:

Action-at-a-Distance: Abuse can be undertaken anytime, anywhere without physical contact (there is a much greater level of flexibility offered in the online environment),

Automation: The use of technology requires less time and environment comparatively speaking to the physical environment,

Accessibility: Due to greater accessibility by many to social media platforms for example, there is a much larger audience to witness the abuse; a source of perhaps greater satisfaction for the perpetrator,

Propagation and Perpetuity: Texts and images can potentially exist for a very long period of time (Fascendini and Fialová, 2011). This factor adds to the potential of leaving an impact, a mark for a long period of time.

According to recent research undertaken by Pew Research Center women are about twice as likely as men to say that they have been targeted as a result of their gender (11% vs. 5%) online (Duggan, 2017). The research also found that women, especially young women face sexualized forms of abuse at much higher rates than men. 21% of women aged 18 to 29 reported being sexually harassed online, a figure that is more than double the share among men in the same age group (9%). In addition, roughly half (53%) of young women ages 18 to 29 have stated that someone had sent them explicit images they did not ask for. As far as the impacts of sexual harassment online are concerned for 35% of women who had experienced any type of online harassment described their most recent incident as either extremely or very upsetting, about twice the share among men (16%). A similar finding has been confirmed by Amnesty International whose 2017 poll found that women are much more likely to experience adverse psychological impacts from online harassment (Banet-Weiser and Miltner, 2016).

The key factors which have led towards online misogyny have been identified by Banet-Weiser and Miltner (2015) as: an outdated view of online spaces such as online games being female free spaces for male nerds; men are threatened by potential economic loss as a result of the apparent feminine invasion

of the online space. There is still a perception of women taking away jobs from men especially in technology fields, recognised as a natural right of men. The critical issue which remains is the non-reporting of such crimes due to negatively impacting factors such as normalisation, fear of not being taken seriously and fear of victim blaming (ibid.)

A comprehensive study of cyber violence and hate speech online against women in the European Union has been undertaken by the European Parliament's Committee on Women's Rights and Gender Equality, published in 2018. The key findings from the report are as follows:

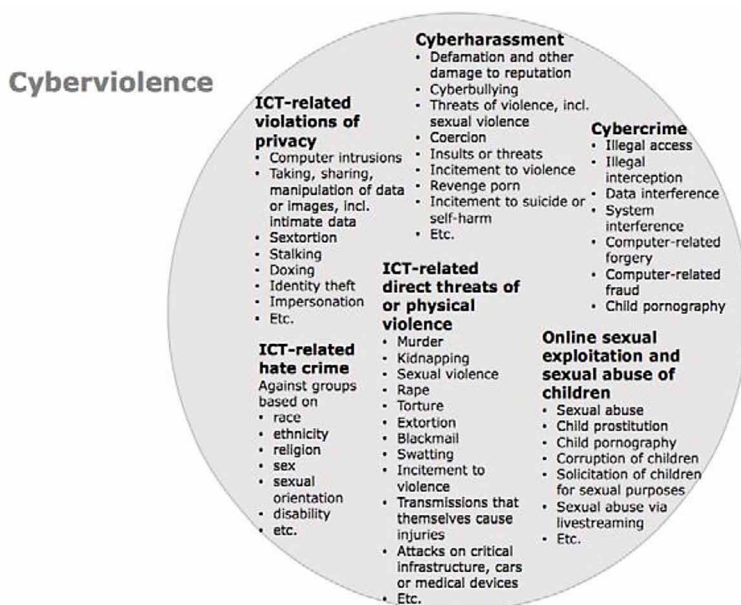
Gender inequality is prevalent in the technology sector and is obvious on platforms and in algorithms, creating toxic techno cultures. The main factors which have contributed to cyber gender inequality and as a result cyber VAWG include the prevalence of anonymity, mob mentality and permanence of negative data with the potential of re-victimisation. Varieties of platforms are used for the purpose of cyber violence and hate speech online. These include social media, web content and discussion sites, search engines, messaging services, blogs, dating websites, apps, comments in media and newspapers, forums and chat rooms of online video games. Online violence can take many forms including sexual harassment, sexual abuse and sexist hate speech with the purpose of discouraging women from public spaces. Legitimation and normalisation of violence against women in the media encourages victim blaming and discouragement of victims' perspectives.

Council of Europe (2018) has captured forms of cyber violence succinctly in the following figure.

As seen in the figure above, cyber violence is a dark side of the Internet. It takes multiple forms from doxing (which is identifying private information about an individual with intent to cause harm) to harassment which covers some very serious issues including revenge porn and issuing threats of violence. Cybercrime is recognised as a category of cyber violence as well as hate-based crimes. In some instances, ICT related acts can be transferred to the physical world resulting in serious crimes including kidnapping, torture, damage to physical assets and other actions against an individual.

Figure 1. Forms of cyber violence

Source: Council of Europe (2018)



Actions which would be considered as cybercrime, which is a step beyond cyber violence have been recognised recently by the European Parliament. Recognition of the large list of actions considered as cyber violence is a strong indication that cyber violence is being seriously considered by governments to undertake steps against in the form of legislation to “punish” acts of cybercrimes. European Parliament (2018) has provided a complete coverage of the types of cybercrimes undertaken against women as:

Violations of Privacy: Revenge porn or image based sexual abuse/ exploitation, creep shots, up skirting or digital voyeurism (the taking of non-consensual photos or videos of women’s private areas and sharing them online,

Doxing: Manipulating and publishing private information without consent,

Impersonation: Stealing identity to threaten or intimidate or to discredit/ damage an individual’s reputation,

Hacking: Intercepting private communications and data for example through webcam hacking.

Cybercrimes Also Include Stalking: Cyber stalking is defined as the action of spying, fixating, compiling information to communicate with individuals against their will.

Harassment which includes cyber bullying is defined as the repeated behaviour using textual or graphical content to frighten or undermine someone’s self-esteem or reputation;

Other Forms of Cybercrime Include Threats of Violence: Rape threats, death threats against the victim, their family members or inciting to physical violence, sending victim unsolicited explicit materials or mobbing: which is defined as choosing or targeting an individual to bully or harass through mob (which includes many individuals) deployment.

Cybercrime has been identified to also include Sexist hate speech which is the use of expressions which spread, incite, promote or justify hatred based on sex. This category also includes posting and sharing of violent content, portrayal of women as sex objects or targets of violence, use of sexist and insulting comments, pushing women to commit suicide in some instances.

Direct violence can also emanate from cyber violence and includes trafficking which is the recruitment and luring of women into prostitution through technology, and the use of stolen graphical content to advertise for prostitution. Sexualised extortion refers to identity theft resulting in physical abuse. And online grooming is the setting up of an online abusive relationship with a minor to bring the child into sexual abuse or child trafficking.

Cyber VAWG and Social Media

There have been numerous criticisms against popular social media platforms such as Facebook for not taking proper action against perpetrators of cyber violence especially in countries such as India where the degree of sexual abuse online and in the real world reaches high levels against vulnerable women and children (Safi, 2017). A report titled “Toxic Twitter” published in 2018 by Amnesty International highlighted the issue that in spite of policies and executives’ concerns Twitter still remains a threatening place for women due to its immediate and direct contact between many users and due to anonymity being its key feature (Amnesty International, 2018).

The attack by bots on women through Twitter is another issue that has been identified (Washington Post, 2018). A well-known example of online hate demonstrated via Twitter was against feminist campaigner and journalist Caroline Criado-Perez (Hardaker and McGlashan, 2016). Criado-Perez’s petition to the Bank of England asked to have Elizabeth Fry’s image on the 5-pound note to be replaced by that of another woman and not Winston Churchill’s as planned (ibid). Criado-Perez faced misogynistic abuse on Twitter. As Hardaker and McGlashan (2016) have found, this case demonstrates the construction

of alternative identities through computer mediated communications as well as social experimentation through cyber misogyny (Baker, 2001). The social experimentation with misogyny which results in harm to others without consequences and accountability utilises the availability of anonymity online.

Anonymity can encourage attitudinal polarisation and a higher likelihood of acting on normally inhibited impulses referred to as deindividualization (Siegel, Dubrovsky, Kilesler and McGuire, 1986). Vinagre (2008) has further classified the misogyny related deindividualization as toxic dis-inhibition. Toxic di-inhibition is demonstrated through rude language, harsh criticisms, anger, hatred, threats, pornography, crime and violence. Harder and McGlashan's (2016) twitter account analysis revealed that sexual aggression (sexist abuse and rape threats) was specifically targeted against women. Men were in most instances constructed as makers and senders of rape threats through social media.

Cyber Violence- Impacts and Consequences

As far as the profiles of women who are specifically targeted online are concerned, the report (European Parliament, 2018) found that young women with intersecting identities are the main targets of online hate crimes as well as women who assert their views online and women in power. Cyber-crimes against women have long term psychological, possibly physical as well as economic impacts for the women, their families and for communities (ibid).

If cyber violence actions remain unaccountable for, without serious consequences for the perpetrator, cyber violence has the potential to create not only serious psychological harm for victims but also negative impacts on *gender equality in virtual and physical environments*. For example, there is currently a dearth of female politicians especially female politicians with inter sectionality characteristics in numerous parts of the world including in economically developed countries such as the United Kingdom. Yet the misogynistic culture of the online environment including its dominance in the social media environment poses a major threat to the progression of women in politics. Cyber-crimes such as harassment, racism and death threats pose a very serious issue of excluding women from a critically impacting and decision-making environment which is also a powerful environment with national and international impacts (Messenger, 2017).

A comprehensive global study on the economic impacts of cyber VAWG has not been undertaken yet but there have been studies on the loss of human capital due to gender inequality to which cyber VAWG contributes immensely. This loss has been estimated at \$160.2 trillion which is twice the value of GDP globally (The World Bank, 2019).

Legal Stance Against Online Misogyny

There have been numerous criticisms of policies and legislations' lack of addressing of online misogyny which has the potential of serious social and economic negative impacts and consequences. Shariff and Eltis (2017) have highlighted the issue of the reluctance of higher education institutions for example not including online forms of sexual violence in the institutions' sexual violence policies. This is in spite of the general trend of millennials and GenZ members being regular users of social media. Shariff and Eltis (2017) have emphasized that the legal system (in this case in the context of Canada) is struggling with how to deal with cases of online sexual violence and that victims do not have trust in the criminal justice system. There is also a serious issue of the legal system assigning blame (by police, prosecutors, defence council and in some instances by judges) to the victims.

Developments in the Legal Systems in Multiple Jurisdictions to Address Online Misogyny

As far as developments in legal systems are concerned, they are still in very early stages. Cyber VAWG presents much more complexity to hold individuals/ parties accountable for cyber VAWG. Different types of resources are required to firstly identify perpetrators. There is a general conception that acts of cyber VAWG can be carried out under the veil of anonymity, without the risk of being identified. There are numerous, complex steps which are required to ensure anonymity online. Otherwise, with the undertaking of big data analysis, by assigning characteristics to individuals, and by combining data available for example profile data on social media, data scientists have been able to accurately (by 90 per cent) identify individuals.

The key factor here is whether resources will be assigned such as paying data scientists to identify perpetrators of cyber VAWG. If cyber VAWG is criminalised formally, then such steps would be required. Regions with considerations for legislation to address cyber VAWG have been identified in literature. They mostly focus on online sharing of images without consent but cyber VAWG legislation is still under development in most parts of the world. Based on the extensive Google search undertaken based on keywords of cyber VAWG (and other associated terms) legislation, multiple regions have been covered. The regions selected are based on the methodology employed by The Guardian for its *Web we want series* investigating the dark side of the Internet (Lyons et al. 2016). Regions prominently covered in other media and reports are also addressed. The following regions are provided as examples where legislation is present or where it is not in existence yet, to address cyber VAWG. Based on this analysis it can be assumed that in spite of the increasing prevalence of cyber VAWG for example in countries like India or China, legislation to address this issue is not comprehensive enough to tackle cyber VAWG effectively. It is important to understand that cyber VAWG legislation is different from VAWG legislation. Multiple countries have legislation to prevent violence against women and girls for example to stop genital mutilation, or sexual harassment in public spaces but cyber VAWG is not addressed by these legislations.

Europe

The Council of Europe (COE) Parliamentary Assembly has recognized the serious negative consequences and impacts of online hate and violence. Resolution 2144 (2017) on ‘Ending cyber discrimination and online hate’ has recognised that sexism and misogyny are types of hate speech and are unacceptable. COE member states have been encouraged to ensure that legislation covers all forms of online violence against a person or a group including the full range of characteristics considered as grounds of protection under discrimination law (Jurasz and Barker, 2017). The Council of Europe has also recognised online misogyny as a major hindrance against the objective of achieving gender equality and has recognised the tackling of cyber gender violence as a key priority (Council of Europe, 2016).

United Kingdom

In the United Kingdom Malicious Communications Act 1988 implies criminal liability for the sending of offensive communications where there is an intention to cause distress or anxiety. It's the application of the Act and the very low percentage of criminal liabilities imposed as a result of cyber violence which has been raised as a serious issue. One of the issues is the degree of thresholds which are applied to recognise an online communication as either abuse or a hate crime (Jurasz and Barker, 2017). Recently, the Law

Commission in the U.K. has stated that the law has failed to keep pace with the dramatic shift in the way society now communicates through online mediums including social media which has brought with it the potential for harm and offence on a massive scale (Hymas, 2018). The Commission has recognised that women are most impacted with misogynistic abuse. The Commission has recommended that online criminal behaviour should be treated the same as in the physical world. And that law for malicious (for example hateful) communications is still ambiguous and needs to be reformed for the purpose of clarity, understandability and effectiveness (Hymas, 2018).

Scotland (Source: Jurasz and Barker, 2017)

Section 127 of the Communications Act 2003 (applicable in Scotland) implies criminal liability for an improper use of a public electronic communications network. Prosecutions made under this provision deal with messages or other matters that are grossly offensive or of an indecent, obscene or menacing character. The section also covers instances of an offence to send or cause to be sent a false message for the purpose of causing annoyance, inconvenience or needless anxiety to another individual.

According to Jurasz and Barker (2017) online text-based abuse should be included in legislation as a criminal offence to reflect other forms of online abuse including image-based sexual abuse. In the context of Scotland, this would imply an amendment to the Abusive Behaviour and Sexual Harm (Scotland) Act 2016. The authors submitted this recommendation to Scottish Parliament's Public Audit and Post-Legislative Scrutiny Committee.

United States

In the United States, Violence against Women Act was passed in 1994 and was further expanded on in the International Violence Against Women Act (I-VAWA), introduced in the U.S. House of Representatives in February 2018 and faces the risk of lapsing in 2018 (Washburn, 2018). The Act has laid the foundations for the Interstate stalking statute and VAWA includes a cyber-stalking provision which can be used against cyber bullying, extortion, defamation, threats, spying, murder, death, serious body injury resulting from digital harassment, surveillance or intimidation (Parra, 2015). The complexities associated with the legislation and the lack of prosecution against online harassment makes it difficult for victims to seek justice in the United States (Carpentier, 2016). There is also a level of ignorance faced by police regarding the serious impacts of cyber VAWG and the civil process ends up being expensive and time consuming to address online harassment (Sweeney, 2014).

Canada

Bill C-13 has been introduced which makes the distribution of intimate images without consent on the Internet a criminal offence (Broadband Commission for Digital Development, 2015).

China

There is no formal legislation to address cyber VAWG in China at present, in spite of it being highlighted as a growing and serious issue for Chinese youth (Lyons and Phillips, 2016).

India

The Indecent Representation of Women (Prohibition) Act 1986 prohibits the indecent representation of women through advertisements, publications, writings, paintings, figures or in any other manner. Any person who violates the provisions of this Act is punishable with imprisonment for a term of two years on first conviction and in the event of subsequent conviction, the imprisonment may extend to five years. To widen the scope of this Act, changes suggested by the National Commission for Women are being examined by the Ministry of Women and Child Development (MWCD) (UN Women, 2016).

The Indecent Representation of Women (Prohibition) Bill 2012 extends the emphasis on portrayal of women in electronic media and electronic modes of distribution of materials. There has been criticism of the term decency and its application in the context of cyber VAWG. At present indecent representation of women is defined as the depiction of the figure or form or body or a part of it of a woman in a way that is indecent, derogatory or denigrating or is likely to deprave, corrupt or injure public morality (Rajagopal, 2017). This definition has been criticised for its ambiguity and more precise understanding of online occurrences, resulting implications of cyber VAWG, including punishments have been asked for.

Russia

Online trolling, especially to promote the government's agenda and to harass anyone trying to stand against the government and authorities as well as to subdue human rights activists is a widespread occurrence in Russia. Gay rights activists are specifically targeted in Russia in the cyber space (Walker, 2016). Understandably, there is no formal legislation for protection against cyber VAWG in Russia.

Colombia-South America

Colombia has had a deep rooted culture of machismo, which rewards hierarchical notions of gender and traditional family roles (Lyons and Phillips, 2016). As a result NGOs especially feminist groups are harassed and threatened not only in the cyber space but also in the physical world. Threats in a lot of cases are followed by physical harm such as sexual assaults of females involved in campaigning for women's rights.

Australia

In Australia, serious cases of abuse through Twitter and Facebook have been punished under the Criminal Code which makes it illegal to menace, harass or threaten through various communications mediums (Farrell, 2016). Two states in Australia, have introduced laws to criminalise the sharing of intimate photos without consent and there has been a Senate committee recommendation to make this a Federal Law.

The Republic of Congo: Africa

Online harassment, cyber VAWG, is not taken seriously in Congo. Females are usually reluctant to report any incidents, yet cyber VAWG is prevalent in the country as is victim blaming (Lyons and Phillips, 2016). Bribery and corruption are also identified as serious issues which act as a barrier to accountability for cyber VAWG in the country.

Summary of Legislation Powers

Based on the analysis above, it appears that in most parts of the world legislation is currently lacking to address cyber VAWG. Even if legislation exists, the complexity of the legislation for example relating to how online communications are treated (harassment versus bullying versus abuse for example) lead towards legal complexities in the court room which can discourage victims of cyber VAWG to report incidents. As literature suggests, victims do not feel confident that bringing to light incidents of cyber VAWG will have any material impact. As the statistics suggest the number of legal cases and the seriousness of punishment for cyber VAWG seem minimal and have been criticised as not being serious enough.

Another issue that has come to light is the lack of awareness and training for law enforcement bodies, which have been grappling with ways to handle situations relating to cyber VAWG. Communications between law enforcers and victims of cyber VAWG have not been perceived as supportive and understanding of the experiences which victims of cyber VAWG have faced. Never the less, international organisations such as the United Nations and UNESCO have provided detailed recommendations to address cyber VAWG.

SOLUTIONS AND RECOMMENDATIONS TO IMPROVE CYBER VAWG RESPONSE

UNESCO (2015) has made the following recommendations for action against cyber VAWG:

Based on the finding that law enforcement agencies and the courts are failing to take appropriate actions for cyber VAWG in 74% of 86 countries surveyed and due to lack of reporting as a result of fear of social repercussions in countries rife with cyber VAWG UNESCO has recommended rigorous oversight and enforcement of rules banning cyber VAWG on the Internet. UNESCO has also, pushed for recognition by governments, regulators, businesses and Internet users that an unsafe Internet implies that women will use the Internet less freely, resulting in costly societal and economic implications. Also, that there needs to be the recognition by internet and social media providers (industry players) of the important role that they play as digital gatekeepers. Industry players include ISPs, mobile phone companies, social networking sites, online dating and gaming sites, website operators and software developers. Tech companies, also as an important industry player, need to recognize cyber VAWG as unlawful behaviour, and need to demonstrate cooperation in providing relief to victims/survivors. They need to focus on better systems for cooperating with law enforcement, more effective takedown procedures for abusive and harmful content, they need to undertake serious consideration of account termination for misconduct and they should produce transparent reports of records specific to cyber VAWG, detailing how and when they have responded (UNESCO, 2015). UNESCO has proposed the three S's which need to work in conjunction with each other: Sensitisation which implies the promotion of changes in social attitudes, Safeguards which cover oversight and monitoring to minimise risks and Sanctions which imply the adoption and application of laws and regulation against cyber VAWG.

Sharriff and Eltis (2017) have suggested that higher education institutions should partner with the justice system, and social media providers and engage the power of students' social media expertise to educate, and sensitise all relevant stakeholders including law enforcement officials. The authors have also recommended raising the standards of online speech and social media activities and recognising online sexual violence as an important element of higher education institutions' sexual violence prevention policies and responses.

The U.K. Government's 2016-2020 strategy has provided this response to addressing cyber VAWG: to address cyber-enabled VAWG by working with the police led Digital Intelligence and Investigation Programme to promote improvements in police capability to investigate online VAWG offences (HM Government, 2016).

European Women's Lobby's (2017) recommendations to address cyber VAWG include:

Policy responses to recognise that cyber VAWG is a type of violence against women and to capture voices of women who are victims of cyber VAWG,

An aim of EU and member states to agree on definitions of forms of cyber VAWG and as a result to include all types of cyber VAWG in legislation As well as to ensure victim access to justice and support services,

Development of legal instruments and policy strategies to punish online VAWG,

An EU Directive and other measures specifically aimed towards addressing VAWG,

To promote improvements in gender dis-aggregated data (including information on sex/gender of the victim, the perpetrator and the relationship) with a focus on the impacts of cyber VAWG, and creating data on the effectiveness of interventions.

Provide support services specifically dedicated to protect women and girls from online violence,

Sustainable funding for such initiatives,

Criminalisation of cyber VAWG,

Training of police, justice systems and professionals to detect, respond and prosecute cyber violence,

The establishment of an independent entity to hear and decide on cyber VAWG cases,

Perpetrators and re-transmitters to be held responsible as well as business entities to respect and remedy human rights through operations,

Internet intermediaries to be held responsible to ensure that platforms are not abused to initiate or maintain cyber violence.

The organisation has also provided recommendations for preventative measures including: adoption of self-regulatory standards to help avoid harmful gender stereotyping and the distribution of degrading images of women or sexual violence imagery. There is also an emphasis on tech companies and internet providers to implement a code of conduct, and gender diversity and equality in the media industry as well as gender training. Also to critically evaluate media information is also proposed. Pornography has been proposed to be recognised as a form of male violence and that opt-in filters should be made available by all internet providers and it is proposed that legislation should limit the distribution of online pornography.

Key action and steps that can be undertaken to tackle cyber VAWG include: development of international policy to recognise cyber VAWG as a crime, to develop international standards to address cyber VAWG through law enforcement agencies as well as greater transparency around cyber VAWG. Transparency should encourage victims of cyber VAWG to report incidents of cyber VAWG to law enforcement bodies and social media platforms should encourage reporting of cyber VAWG. Awareness and education programs need to be undertaken with a specific focus on cyber VAWG, targeting young men and boys to influence behavioural change. Respect in communications can be one element that initiatives around education and awareness can encompass. Education around breaking away from stereotypes of women as sexual objects, weak, something that can be easily abused or men being the more powerful gender (misogynist stereotyping) is critical to implement change towards addressing cyber VAWG.

FUTURE RESEARCH DIRECTIONS

This chapter has laid the foundation for understanding cyber VAWG. It has also provided a brief understanding of the impacts of this cybercrime as well as the legal stance on cyber VOWG. Future research should look at evaluating actual changes which are taking place in legislation, in enforcement mechanisms and expert views on whether these measures are adequate or whether they require further action and the types of strategies which can be adopted. Types of social changes which need to occur but are hard to implement in this space need to be evaluated, also from organisations and systems perspectives. There is a very large potential in this space for further research, also from country and jurisdiction specific perspectives.

CONCLUSION

Cyber VAWG is a recent phenomenon, allowed by affordance of misogynistic behaviours through the Internet; which has potentially serious implications including the extension of online violence to the physical environment. It is the case of online misogyny which jurisdictions around the world are trying to firstly accurately define and secondly aiming to create adequate legislation and its enforcement to address. As demonstrated in the multi-regional coverage of legislation, legislative developments against cyber VAWG are still in infancy or do not exist in many countries.

There is a large amount of work which needs to be undertaken to tackle cyber VAWG, at various levels of legislation development, enforcement and social change. A critical issue which needs high level (international) attention is the risk and danger which online misogyny poses from various perspectives including the exclusion of females from the Internet. Internet is a powerful instrument of communication and change and tackling online misogyny is an important factor towards promoting gender empowerment and promotion of human rights online. As discussed above there are various recommendations which have been provided but it is their actual implementation in the form of action for example in the form of punishment for online misogyny or social media providers' implementation of a code of conduct which need to occur. Implementing accountability to tackle cyber VAWG and to make the internet a safe space is critical for female empowerment and gender equality in the Internet environment.

REFERENCES

- Alvares, C. (2018). Online staging of femininity: Disciplining through public exposure in Brazilian social media. *Feminist Media Studies*, 1–18.
- Amnesty International. (2018). *Toxic Twitter - A Toxic Place For Women*. Retrieved 10th of October 2018 from <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>
- Baker, P. (2001). Moral panic and alternative identity construction in Usenet. *Journal of Computer-Mediated Communication*, 7(1).
- Banet-Weiser, S., & Miltner, K. M. (2016). # MasculinitySoFragile: Culture, Structure, and Networked Misogyny. *Feminist Media Studies*, 16(1), 171–174. doi:10.1080/14680777.2016.1120490

Broadband Commission for Digital Development. (2015). *Cyber violence against women and girls*. Retrieved 10th of October 2018 from <https://en.unesco.org/sites/default/files/genderreport2015final.pdf>

Carpentier. (2016). *Online abuse: how different countries deal with it*. Retrieved 10th of October 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrasment-revenge-pornography-different-countries-deal-with-it>

CEDAW. (1992). *General Recommendation No. 19*. Retrieved 10th of October 2018 from <http://www.refworld.org/docid/52d920c54.html>

CEDAW. (2017). *General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19*. Retrieved 10th of October 2018 from https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf

Christina, G. (2012). *#mencallmethings: 'FUCKIN HOE,' 'FUCKIN FEMINAZI SLUT.'* Greta Christina's Blog: Atheism, sex, politics, dreams, and whatever, August 8. Retrieved 10th of October 2018 from <https://the-orbit.net/greta/2012/08/27/mencallmethings-old-bag/>

Cole, K. K. (2015). It's like she's eager to be verbally abused: Twitter, trolls, and (en) gendering disciplinary rhetoric. *Feminist Media Studies*, 15(2), 356–358. doi:10.1080/14680777.2015.1008750

Council of Europe. (2016). *Combating sexist hate speech*. Retrieved 10th of October 2018 from <https://edoc.coe.int/en/genderequality/6995-combating-sexist-hate-speech.html>

Council of Europe. (2018) *CyberCrime Convention Committee, Working Group on cyber bullying and other forms of online violence, especially against women and children (CBG), "Mapping study on cyber violence"* (Draft). Retrieved 10th of October 2018 <https://rm.coe.int/t-cy-2017-10-cbg-study/16808b72da>

Doyle, S. (2011). But How Do You Know it's Sexist? The #MenCallMeThings Round-Up. *Tiger Beatdown*. Retrieved 10th of October 2018 from <http://www.tigerbeatdown.com/2011/11/10/but-how-do-you-know-its-sexist-the-mencallmethings-round-up/>

Duggan, M. (2017). *Online harassment 2017*. Retrieved 10th of October 2018 from <http://www.pewinternet.org/2017/07/11/online-harassment-2017/>

European Parliament. (2018). *Cyber Violence and hate speech online against women Study for the FEMM Committee*. Retrieved 12th of November 2018 from [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU\(2018\)604979_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf)

European Women's Lobby. (2017) *#HerNetHerRights Resource Pack on ending online violence against women & girls in Europe*. Retrieved 12th of November 2018 from https://www.womenlobby.org/IMG/pdf/hernetherights_resource_pack_2017_web_version.pdf

Farrell, P. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrasment-revenge-pornography-different-countries-deal-with-it>

Fascendini, F., & Fialová, K. (2011). *Voices from digital spaces: Technology related violence against women*. Association for Progressive Communications. Retrieved 12th of November 2018 from https://www.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0_0.pdf

Government, H. M. (2016). *Ending violence against women and girls, Strategy 2016-2020*. Retrieved 12th of November 2018 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/522166/VAWG_Strategy_FINAL_PUBLICATION_MASTER_vRB.PDF

Hardaker, C., & McGlashan, M. (2016). Real men don't hate women: Twitter rape threats and group identity. *Journal of Pragmatics*, 91, 80–93. doi:10.1016/j.pragma.2015.11.005

Hess, K., & Waller, L. (2014). The Digital Pillory: Media Shaming of 'Ordinary People for Minor Crimes. *Continuum*, 28(1), 101–111. doi:10.1080/10304312.2013.854868

Hymas, C. (2018). *Legal system fails to protect women from online abuse, says Law Commission*. Retrieved 12th of November 2018 from <https://www.telegraph.co.uk/news/2018/11/01/legal-system-fails-protect-women-online-abuse-says-law-commission/>

Jurasz, O., & Barker, K. (2017). Submission of Evidence to Scottish Government Independent Review of Hate Crime Legislation (Bracadale Review). *Independent Review of Hate Crime Legislation in Scotland*. Retrieved 12th of November 2018 from <http://oro.open.ac.uk/52612/1/Hate%20Crime%20Legislation%20Review%20%28Barker%20%26%20Jurasz%29.pdf>

Lyons, K., & Phillips, T. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>

Lyons, K., Phillips, T., Walker, S., Henley, J., Farrell, P., & Carpentier, M. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>

Manne, K. (2018). *Living in a man's world: the logic of misogyny*. Available at <https://global.oup.com/academic/product/down-girl-9780190604981?cc=au?lang=en?&lang=en&>

Ottawa Coalition to End Violence Against Women. (2016). *Cyber violence*. Retrieved 12th of November 2018 from <https://techwithoutviolence.ca/cyberviolence>

Parra, E. (2018). *The path to cyber stalking laws tied to the First State Delaware Online*. Retrieved 12th of November 2018 from <https://www.delawareonline.com/story/news/local/2015/06/13/path-cyberstalking-laws-tied-first-state/71179794/>

Rajagopal, K. (2017). *Update for the online era*. Retrieved 12th of November 2018 from <https://www.thehindu.com/opinion/op-ed/update-for-the-online-era/article19729572.ece>

Safi, M. (2017). Facebook allowed child abuse posts to stay online for more than a year, Indian court hears. *The Guardian*. Retrieved 12th of November 2018 from <https://www.theguardian.com/world/2017/nov/03/facebook-allowed-child-abuse-posts-stay-online-year-indian-court-hears>

Shariff, S., & Eltis, K. (2017). Addressing Online Sexual Violence: An Opportunity for Partnerships between Law and Education. *Education Law Journal*, 27(1).

Siegel, J., Dubrovsky, V., Kiesler, S., & McGuire, T. W. (1986). Group Processes in Computer-Mediated Communication. *Organizational Behavior and Human Decision Processes*, 37(2), 157–187. doi:10.1016/0749-5978(86)90050-6

Stanton, C. (2011). Here's a project: Troll! Data! Analysis! *SuperOpinionated*. Retrieved 12th of November 2018 from <http://superopinionated.dreamhosters.com/2011/02/08/here-is-a-project-troll-data-analysis>

Swaminathan, R. (2014). Politics of Technoscapes: Algorithms of Social Inclusion & Exclusion in a Global City. *Journal of International & Global Studies*, 6(1), 90-105. Retrieved 12th of November 2018 from <http://www.lindenwood.edu/files/resources/90-105.pdf>

Sweeney, M. (2014). *What the Law Can (and Can't) Do About Online Harassment*. Retrieved 12th of November 2018 from <https://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/>

The World Bank. (2018). *Unrealized Potential: The High Cost of Gender Inequality in Earnings*. Retrieved 12th of November 2018 from <https://www.worldbank.org/en/topic/gender/publication/unrealized-potential-the-high-cost-of-gender-inequality-in-earnings>

UN Broadband Commission for Digital Development Working Group on Broadband and Gender. (2015). *Cyber Violence Against Women and Girls A World-Wide Wake-Up Call*. Retrieved 12th of November 2018 from <https://en.unesco.org/sites/default/files/genderreport2015final.pdf>

UN Women. (2016). *Indecent representation of women (Prohibition) Act*. Retrieved 12th of November 2018 <http://evaw-global-database.unwomen.org/en/countries/asia/india/1986/indecent-representation-of-women--prohibition--act-1986>

UNESCO. (2015). *Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call Highlights*. Retrieved 12th of November 2018 from <https://en.unesco.org/sites/default/files/highlight-documentenglish.pdf>

Valenti, J. (2014). *Jessica Valenti's Facebook Page, last modified June 30*. Retrieved 12th of November 2018 from https://www.facebook.com/permalink.php?story_fbid1/410152263488833160&id1/4360994083159

Vinagre, M. (2008). Politeness strategies in collaborative e-mail exchanges. *Computers & Education*, 50(3), 1022–1036. doi:10.1016/j.compedu.2006.10.002

Walker, S. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>

Washburn, K. (2018). *Violence Against Women Act at risk of lapsing*. Retrieved 12th of November 2018 from <https://www.opensecrets.org/news/2018/10/vawa-at-risk-of-lapsing/>

Zimmerman, A. G. (2012). *Online Aggression: The Influences of Anonymity and Social Modelling*. University of North Florida. Retrieved 12th of November 2018 from <https://digitalcommons.unf.edu/cgi/viewcontent.cgi?article=1472&context=etd>

Intimate Partner Cyber Abuse Viewed Through the Lens of Criminology

Curtis L. Todd

Atlanta Metropolitan State College, USA

Joshua E. Byrd

American Intercontinental University, USA

Leroy Baldwin

Atlanta Metropolitan State College, USA

INTRODUCTION

The field of Criminology covers all areas of criminal justice systems – law enforcement, the courts and corrections. Governing policies and protocols of these coordinated networks, from controlling crime, adjudication to imposing penalties on those who violate laws, are often informed by social scientific inquiry and have far reaching implications beyond academia.

Intimate Partner Cyber Abuse is an area that should now figure prominently, not only as a research target among criminal justice scholars, but also among practitioners. It is the new looming frontier that local, state, national and international criminal justice jurisdictions and other stakeholders grapple with in efforts to effectively hold offenders accountable and to support victims of this kind of abuse being perpetrated via technological structures. The pervasive and anonymous nature of the Dark Web fosters the ideal environment where Intimate Partner Cyber Abuse can go undetected due to the absence of standard regulatory oversight and laws.

In addition to confronting this emerging frontier, there is a need to interrogate the crevices between where criminal justice systems are – with respect to Intimate Partner Cyber Abuse – and the advances that need to occur to ensure appropriate and effective responses across all systems. To that end, the purpose of this chapter is to significantly assist in filling these problematic gaps. Key concepts are first contextually defined to establish a clear understanding of the complex issues associated with Intimate Partner Cyber Abuse. Additionally, gateways to abuse and exploitation, as well as protective strategies, and inherent implications are examined to fully explicate the importance of refocusing this issue through a criminological lens. Data and relevant literature are also mined to provide thoughtful and robust suggestions and recommendations. Finally, future research directions are presented.

BACKGROUND

Criminology is the scientific study of how laws are made, those who break them and how the criminal justice system responds to them (Sutherland & Cressey, 1960). The landscape it examines has grown exponentially since the inception of the internet. With this expansion has come new tools for criminality and new ways in which crime and violence can occur. The unprecedented growth which has taken place

DOI: 10.4018/978-1-5225-9715-5.ch041

on the World Wide Web has given birth to a digital Pandora's Box called the Dark Web, where many facets of cybercrime, such as violence and victimization, occur at alarming rates which includes cyber abuse among intimate partners. In simplistic terms, the Dark Web can be defined as the problematic facet of the Web associated with cybercrime, hate, and extremism (Fu, Abbasi, & Chen, 2010). The undetectable and often impenetrable nature of the cyberspaces where these crimes occur are referred to as "the deep web" and it is here where cybercriminals identify their targets and carry out their unlawful agendas. The complexities associated with this new terrain has created a "perfect storm" that has yet to be fully understood. Moreover, these challenges have brought with them new predatory criminals such as cyberbullies and abusers. New criminals who launch attacks from cyberspace are technologically savvy and seemingly operate in a world where laws and meaningful oversight have not kept pace with the rapid growth of the web, nor the myriad of ways in which it has been weaponized to advance personal, social, political and economic agendas. They use the far-reaching tools of the digital world to exact violence upon their victims whether they be strangers or intimate partners.

INTIMATE PARTNER CYBER ABUSE

The operational definition of Intimate Partner Cyber Abuse is framed through a bifurcated lens that explicates the terms "intimate partner" and "cyber abuse." The Center for Disease Control and Prevention, National Center for Injury Prevention and Control's publication "Intimate Partner Violence Surveillance: Uniform Definitions and Recommended Data Elements, Version 2.0," which was authored by Breiding et al (2018) endeavored to promote, as well as improve consistency in which Intimate Partner Violence is surveilled across organizations and among stakeholders seeking to address this problematic social issue. The definition of intimate partner, among other critical descriptions included in the publication, notes:

An intimate partner is a person with whom one has a close personal relationship that may be characterized by the partners' emotional connectedness, regular contact, ongoing physical contact and sexual behavior, identity as a couple, and familiarity and knowledge about each other's lives. The relationship need not involve all of these dimensions (p. 11).

Further, a defining feature of intimate partner includes current or former relational characterizations such as spouses, boy and girl friends, dating partners or ongoing sexual partners. They can be in an opposite or same sex relationship. They may be living together or not. It is also important to note that an intimate partnership need not require sexual intimacy (Smith, et al, 2018).

Intimate abuse, due to its seriousness, is frequently captured in the literature alongside the terms such as intimate violence, relationship violence, and domestic violence. Therefore, to further operationalize Intimate Partner Cyber Abuse, the definition of abuse is drawn from a seminal report by the Working Group on Intimate Partner Abuse and Relationship of the American Psychological Association. The Group (2002) concluded:

Abuse usually includes an ongoing pattern of behavior, attitudes, and beliefs in which a partner in an intimate relationship attempts to maintain power and control over the other through the use of psychological, physical and/or sexual coercion. Abuse usually produces fear and trauma in those being victimized, whereas isolated aggressive acts may not (p.3).

Therefore, Intimate Partner Cyber Abuse is characterized by online behaviors that threaten, intimidate, harass, humiliate or harm a person involved in a close personal relationship with another person in which they are described as being a couple due to their relationship meeting certain conditions such as emotional connection, regular contact, and ongoing physical contact that need not be sexual.

It was only a matter of time before social interaction in virtual landscapes would evolve into intimate partnerships. These cyber relationships present a myriad of opportunities when they escalate into abuse perpetrated either exclusively online or in the physical world. At times, the impetus and continuation for some of these relationships is fraud, and has become known as Online Romance Scams (Whitty & Buchanan, 2012). Another form of fraud that has increased over the years in an activity known as “catfishing,” which involves perpetrators posting false information, profiles, and at times photographs, with the sole purpose to intentionally manipulate, mislead, or harm others. Unfortunately, computers and technological advances have afforded growing avenues and opportunities for abuse to include cyber exploitation, intimidation, stalking and psychological aggression. Due to easily acquired levels of anonymity, the capricious nature of cyberspace and perpetrators not needing a geographical locale, variances in Intimate Partner Cyber Abuse easily expands in its frequency and severity.

For the purpose of this chapter, Intimate Partner Cyber Abuse, focuses on relationships that are initially forged online and the abuse is perpetrated via technological structures and social media networking platforms to include email, apps, twitter, instagram, snapchat, tumblr and the like. The definition is inclusive of relationships that transitions to the physical world. Further, a rise in what is being referred to as digital domestic violence and digital abuse is now on the radar. This abuse also includes the use of texting, as well as smart technology such as internet-connected locks, thermostats, lighting and cameras through smartphone apps connected to internet-enabled devices (Bowles, 2018). All of these acts are meant to further harass, monitor, and control intimate partners. Caution must be also taken not to be dismissive of other digital landscapes in which abuse could occur which might be evolving or existing in the margins, away from mainstream online platforms.

Gateways to Cyber Abuse

The term ‘gateway’ has been traditionally associated with drugs usage and the theory that such use increases the probability of the user engaging in other further drugs. The ideology is also analogous to marijuana being designated as a gateway to more dangerous drugs, therefore protective factors need to be strengthened and risk factors mitigated as it relates to cyber abuse, generally and specifically among intimate partners. Numerous pathways lead to the Dark Web, “Big Box” websites and social media platforms provide the nexus which links users of all ages to a frontier society eerily similar to the days of the “wild west” in the western world, where law enforcement was virtually nonexistent and occurrences of violence and crime were abundant. It is within this framework that well intended users who hold naive assumptions learn to navigate this burgeoning digital world which seems to find a way to entangle all who enter.

Within moments of visiting “Big Box” social media platforms, like Facebook and Instagram, then establishing a user profile and going live with their account, members of cyberspace can quickly find themselves in an unintended relationship. Beginning with the preverbal “handshake” which is achieved by liking a post, picture or video, intimate relationships in cyberspace quickly progresses. In the cyber world, liberal norms mixed with a lack of professional digital decorum, ultimately mold relationships into unrealistic, unattainable and oftentimes deceptive illusions, almost from their inception. The creation

and evolution of these relationships often move as fast as the high speed digital highway will allow, advancing the stages of such relationships by the click of a mouse.

Protective Strategies

Protective factors or strategies is a wide-ranging catchphrase used to advance the idea that informed and planned measures can be employed to prevent the occurrence of an undesired outcome. To that end, various tactics have been suggested to address the dangers of interacting with others in cyberspace, but without comprehensive solutions comprised of international alliances, the prospects of curbing instances of Intimate Partner Cyber Abuse and related violence show little promise. Some promising well intended efforts are underway, but to be effective, the strategies employed should be inclusive of fair and balanced frameworks. Such measures should also be lenient, flexible enough to provide space for free communications and rigid enough to protect the interest and safety of would be cyber abuse victims. In North Carolina, courts decided the state went too far in addressing cyber violence when it enacted a 2009 law focused on curbing cyber bullying. They argued the law reached too far in prohibiting certain uses of computers and that would encourage or show purposeful intimidation of others online.

Other efforts can be seen internationally. Consider China as a case study. In China, nearly every digital interaction is captured and stored in a database linked to an individual's social credit score. This database, one of the largest social engineering projects ever attempted, aims to monitor the actions of China's entire population, over a billion people, by maximizing the technological advances of the internet and its tools. The success of China's system has yet to be determined; nevertheless we know that China's approach, though well intended, may go too far in restricting personal freedoms in other countries.

Macro level approaches to address Intimate Partner Cyber Abuse may also serve as successful strategies. In the United States, the Centers for Disease Control and Protection (CDC) recommends teaching healthy relationship skills as a means of reducing risk and incidences of intimate partner abuse (Centers for Disease Control, 2017). Similar recommendations have also been suggested in Canada where teaching basic behaviors like respect and responsibility have been offered as strategies to protect children from cyber abuse (Broll 2018). A public health approach, which focuses on harm prevention and reduction by identifying risk and protector factors, has immense currency in safe guarding individuals and the larger society against someone becoming a victim or a perpetrator of Intimate Partner Cyber Abuse.

Protection Orders and Other Legal Remedies

Employing legal avenues as a response to cyber abuse can be expensive and time consuming. However, it is an important step that needs to be taken in holding perpetrators accountable. Further, legal remedies also offer a measured attempt to reclaim ones dignity, value as a human being and engenders a sense of empowerment. Traditional protection efforts are found in instances of domestic violence with attempts to remedy abuse through the following: Emergency Protection Orders, Protection Orders and Restraining Orders. An Emergency Protection Order can be given by a police officer in some states. The Order, which is generally limited to no more than a week, is given when the abuser is arrested for domestic violence. It is also typically given by a magistrate. A Protection Order ranges from one to five years and can last up to a lifetime. This type of protective order can be found in each of the 50 states in America, as well as in the District of Columbia. There are also different provisions in a Protection Order such as no contact, move out and in some cases a counseling provision. Last, a Restraining Order differs from the aforementioned orders in that it requires individuals in a lawsuit to do or not do certain

things, usually stemming from case related situations such as divorce, civil or other family cases (Find Law, 2018). When Intimate Partner Cyber Abuse is perpetrated, these efforts can fall short as protective legal remedies against abuse because they do not go far enough in covering potential acts executed via technological structures.

While every case of Intimate Partner Cyber Abuse is different, seemingly, there has been a near collective effort in the United States to address the issue of revenge porn, also known as nonconsensual pornography, which is among the most deleterious type of cyber abuse. Forty states and the District of Columbia now have revenge porn laws (Cyber Civil Rights Initiatives, n.d.). Some states have measures that include specific language such as cyber harassment statutes, cyberbullying policies, cyberstalking, harassment by telecommunication device, state online harassment, obscene electronic communications, computer crime, and harassment by computer laws. Other state laws have attempted to cover acts like revenge porn under existing harassment statutes.

SOLUTIONS AND RECOMMENDATIONS

As with most crime, addressing criminality such as Intimate Partner Cyber Abuse is a moving target that keeps pace with technological advancements in cyberspace. The nature of these changes and the continued growth of internet users, websites, apps and messaging platforms make it nearly impossible for law enforcement to sufficiently address this crime and hold criminals accountable for their abuse. There are however, strategies that can be implemented which may prove successful in decreasing the prevalence and pain resulting from such abuse and proposed processes for resolutions to make abuse victims whole. In addition to not sharing private data and reporting instances of abuse, the following proposed recommendations go above and beyond common best practices for internet users.

- Define and elevate Intimate Partner Cyber Abuse to priority status to be addressed by politicians, practitioners, police and private citizens.
- A robust research agenda needs to be developed to investigate the prevalence, correlates, and consequences of Intimate Partner Cyber Abuse, nonconsensual pornography and other related abuses (Eaton, Jacobs, & Ruvalcaba, 2017).
- Create international legal frameworks as recommended by the American Civil Liberties Union (ACLU) and other free-speech groups devoted to providing uniformity of cyber laws aimed at penalizing those who post false information via digital tools and techniques to intentionally manipulate, mislead, or harm others.
- Hold Internet providers accountable for providing strict account authentication procedures for those who use their services and require account holders to follow specific rules while using the internet.
- Require mandatory cyber training for law enforcement personnel and educators which also focuses on Intimate Partner Cyber Abuse.
- Provide more efficient methods of approving video and photo uploads to minimize the psychological harm inflicted upon those who approve the publishing of online videos and photos such as what was referenced in “The Cleaners,” a documentary film that addressed the psychosocial harm suffered by employees who monitor, sift through and remove inappropriate content on the Internet for “Big Box” social media networks.

- Create a credit scoring system for online behavior similar to China's new Social Credit System. Just as an individual's personal credit score can fluctuate depending upon their business relationships, a person's social score should adjust similarly in response to their online behavior. For example, a person's social credit score would decrease if they are found guilty of posting fake news online, catfishing or cyber abuse.

Finally, there is an overwhelming need to also educate national and international groups that occupy influential spaces regarding the presence and rise in this type of abuse. Criminal justice system networks must remain proactive, rather than relying on reactive posturing as it relates to legal remedies. Greater effort is needed in educating individuals of their rights and applicable laws when they have been abused. This can be achieved through Intimate Partner Cyber Abuse awareness campaigns from victim assistance programs, advocacy groups and public service announcements across all media platforms, especially the web, which is "ground zero" for this issue.

FUTURE RESEARCH DIRECTIONS

The colloquial expression, "the train has left the station," is instructive when considering the breadth and depth of exploration needed to fully realize current and future issues related to the varied aspects of cybercrime. It is a new frontier and Intimate Partner Cyber Abuse figures prominently. The following recommendations for future research directions, though not exhaustive, provide a thoughtful thematic structure and agenda useful in closing gaps regarding where we are and where we should be to effectively address Intimate Cyber Partner Abuse.

- Greater gatekeeping measures need to be comprehensively examined in efforts to provide informed prevention strategies to counter predatory and abusive behavior.
- Research initiatives must specifically target cyber monitoring practices pertaining to "age related" and "time spent online" behavior as a means to protect vulnerable populations.
- Cyber privacy and protection can be strengthened through social scientific research and can garner additional policies, procedures and protocols useful for the public and private sectors.
- Ongoing methods to determine the effectiveness of existing laws must include longitudinal studies. A review over time has immense utilitarian purposes in determining what is and is not working to counter cyber abuse.
- Scientific inquiry that explores the role of criminal justice systems (law enforcement, courts, corrections) and their response to cyber abuse should be an ongoing endeavor to ensure updated and relevant information and practice standards.

CONCLUSION

There is an abundance of research on the harmful nature of intimate partner abuse and its impact on those victimized by offenders. Further, though best practice standards in assisting abuse victims continue to evolve, there is much more work to do in our understanding of this issue and ability to appropriately address the social, emotional and psychological impact of Intimate Partner Cyber Abuse. Understanding the complex nature of this type of abuse is an important first step in providing holistic remedies. Criminal

justice educators, researchers and practitioners are uniquely positioned on the frontline of identifying problematic and criminal behaviors, proposing solutions and recommendations, as well as directing future social scientific inquiry. Intimate Partner Cyber Abuse is now on our collective radar and its impact on individuals cannot be minimized. As the digital world continues its rapid expansion, keeping pace with it must be matched with aggressive strategic measures from criminal justice networks, both nationally and internationally. This includes robust examination and monitoring of technological gateways that lead to abuse, as well as developing protective strategies informed by research. Finally, within the same mindset, legal remedies and provisions must not be allowed to wane or lag. The assertiveness that is being employed by intimate partner cyber abusers must be met with the full authority of criminal justice systems which are committed to conquering this new frontier that also ensure that survivors, as much as possible, are made whole.

REFERENCES

- Bowles, N. (2018, June 23). Thermostats, locks and lights: Digital tools of domestic abuse. *New York Times*. Retrieved from <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>
- Breiding, M. J., Basile, K. C., Smith, S. G., Black, M. C., & Mahendra, R. R. (2015). *Intimate partner violence surveillance: Uniform definitions and recommended data elements, Version 2.0*. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.
- Broll, R. (2018). Cyberbullying: Four steps to protect your kids. *The Conversation*. Retrieved from <https://theconversation.com/cyberbullying-four-steps-to-protect-your-kids-90907>
- Cyber Civil Rights Initiative. (n.d.). *40 states + DC now have revenge porn laws*. Retrieved from <https://www.cybercivilrights.org/revenge-porn-laws/>
- Domestic violence: Orders of protection and restraining orders. (2018). Retrieved from <https://family.findlaw.com/domestic-violence/domestic-violence-orders-of-protection-and-restraining-orders.html>
- Eaton, A. A., Jacobs, H., & Ruvalcaba, Y. (2017). *2017 Nationwide online study of nonconsensual porn victimization and perpetration: A summary report*. Cyber Civil Rights Initiative. Retrieved from <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>
- Smith, S. G., Zhang, X., Basile, K. C., Merrick, M. T., Wang, J., Kresnow, M., & Chen, J. (2018). *The national intimate partner and sexual violence survey (NISVS): 2015 data brief*. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.
- Sutherland, E., & Cressey, D. (1960). *Principles of criminology* (6th ed.). Philadelphia: J.B. Lippincott.
- Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 181–183. doi:10.1089/cyber.2011.0352 PMID:22304401
- Working Group on Intimate Partner Abuse and Relationship. (2002). Intimate partner abuse and relationship violence. *American Psychological Association*. Retrieved from <https://www.apa.org/about/division/activities/partner-abuse.pdf>

ADDITIONAL READING

Centers for Disease Control. (2017). *Preventing intimate partner violence*. Retrieved from <https://www.cdc.gov/violenceprevention/pdf/ipv-factsheet.pdf>

Chisolm, D. (2018, Jun 29). Why we need revenge porn safeguards [Video file]. Retrieved from <https://www.youtube.com/watch?v=C2a1AWdsUPI>

Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Thousand Oaks, CA: Corwin.

Marganski, A., & Melander, L. (2018). Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence*, 33(7), 1071–1095. doi:10.1177/0886260515614283 PMID:26611614

Patchin, J. W., & Hinduja, S. (2018). Sextortion among adolescents: Results from a national survey of U.S. youth. *Sexual Abuse*. doi:10.1177/1079063218800469 PMID:30264657

Riesewieck, M., & Block, H. (Directors). (2018). *The cleaners* [Documentary]. Independent Lens. PBS. Retrieved from <http://www.pbs.org/independentlens/films/the-cleaners/>

Wolford-Clevenger, C., Zapor, H., Brasfield, H., Febres, J., Elmquist, J., Brem, M., ... Stuart, G. L. (2016). An examination of the Partner Cyber Abuse Questionnaire in a college student sample. *Psychology of Violence*, 6(1), 156–162. doi:10.1037/a0039442 PMID:27014498

KEY TERMS AND DEFINITIONS

Catfishing: Using digital tools and techniques to post false information, profiles, and or photographs with the sole purpose of intentionally manipulating, misleading, or harming others.

Criminology: The critical and systematic examination of how laws are made, the means, modes and motives of criminal offenders, and the collaborative responses to criminal activities by the judicial system, policy makers and community stakeholders.

Cyber Abuse: Online behavior that threatens, intimidate, harass, harm, or humiliate a person.

Cyberbullying: The act of bullying by employing tools available on electronic devices which connect to the internet, messaging services, and others digital communication networks.

Cybercrime: The violation of law on internet platforms (or in cyberspace) by incorporating internet tools and electronic devices such as phones and computers.

Dark Web: Areas in cyberspace operating outside of the purview of law enforcement and internet regulations which provide ample opportunities for digital criminal enterprises to exist.

Gateways to Cyber Abuse: Computer applications or apps, websites, social media networks, texting services and other communication modes which can digitally or electronically connect users to cyberspace (the internet).

Intimate Partner: A close personal relationship between individuals who identify as a couple that is characterized by some of the following dimensions: emotional connection, regular contact, and ongoing physical contact that need not be sexual.

Nonconsensual Pornography: The distribution of sexually graphic images, including through digital platforms, of individuals without their consent. This is also referred to as “revenge porn,” “cyber rape,” and “involuntary porn.”

The Dark Side of Engaging With Social Networking Sites (SNS)

3

Eileen O'Donnell*Technological University Dublin, Ireland***Liam O'Donnell***Technological University Dublin, Ireland*

INTRODUCTION

Although engagement with the deep or dark web may seem to some to be intimidating or possibly threatening, the surface web similarly presents users with challenges which may also be detrimental to one's peace of mind or health. This paper reviews the dark side of engaging with the surface web through the use of Social Networking Sites (SNS), the issues discussed in this paper will also be relevant to users' engagement with the deep and dark web. While SNS have the potential to impact positively on adolescent's health and well-being, the use of SNS has the potential for exposure to possible risks (Guinta & John, 2018). SNS include: Facebook (2018), QZone (2018), YouTube (2018), Twitter (2018), Reddit (2018), Pinterest (2018), Tumblr (2018), Flickr (2018), Whatsapp (2018), Snapchat (2018), Viber (2018), Google+ (2018), Instagram (2018), LinkedIn (2018), Skype (2018), Tinder (2018), Grindr (2018), amongst many others used around the world. Computer algorithms are used to draw people in to frequent use of SNS. Once someone is online and engaging with SNS, more computer algorithms are used to keep the persons attention and hence increase the amount of time spent online. Recommender systems are used to enhance collaborative filtering algorithms which encourage users engagement with Social Networking Sites (Eirinaki, Gao, Varlamis, & Tserpes, 2018; Liu & Lee, 2010). The dark side of engaging with SNS includes: addiction or addictive behavior, child pornography, cyberbullying, fake news, Fear Of Missing Out (FOMO), social comparisons, stalking, amongst many others, which can all lead to neglect of other duties, sleep deprivation, loneliness, isolation, depression, and so forth. The aim of this chapter is to review the negative effects of engaging with SNS and consider what solutions can be proposed to alleviate the damage caused by engagement with SNS.

BACKGROUND

"It is increasingly observable that social media present enormous risks for individuals, communities, firms, and even for society as a whole" (Baccarella, Wagner, Kietzmann, & McCarthy, 2018, p. 431). Now that we as a society are aware of the possible dangers posed by social media, it is time to address all of these potential risks with individuals, communities, organisations, and so forth. By identifying and highlighting these risks and through ensuring that individuals, communities, and organisations are made aware of these risks, only then will it be possible to successfully deal with such risks. "Even with social media executives admitting that their platforms have deleterious impacts, users tend not to question the short- and long-term implications and potential risks of their choices" (Baccarella et al.,

DOI: 10.4018/978-1-5225-9715-5.ch042

2018, p. 432). Users should be encouraged to question the short and long term risks of engaging with SNS. This is a discussion in which all members of society should engage, not just parents and school teachers. Many adults are experiencing problems as a result of excessive engagement with SNS. This paper reviews some of the negative effects of engaging with SNS on the habits (addiction and addictive behaviour, exposure to child pornography, cyberbullying) and mental health (fake news, fear of missing out, social comparisons, stalking) of users. In addition, users are encouraged to consider how their use of SNS may be impacting the lives of others (family members, work colleagues, and other online users).

The Dark Web

The dark web represents a number of anonymously created websites which are hosted on the deep web. The dark web is intentionally hidden (Paul, 2018), the content is not indexed for search engines to find, unlike the surface web where the content is indexed and accessible to standard web browsers, for example, Google Chrome (Google, 2019), Mozilla Firefox (Firefox, 2019), or Microsoft Internet Explorer (Microsoft, 2019). The surface web is the opposite of the deep web (also known as the invisible web and the hidden web). The surface web is easily accessible to all using standard web browsers on the internet. The deep web and the dark web are not accessible through standard web search engines and web crawlers.

In a research study conducted by Dalins, Wilson & Carman (2018) the findings suggest that “criminality on this ‘dark web’ is based more upon greed and desire, rather than any particular political motivations” (Dalins et al., 2018, p. 62). The dark web refers to a number of anonymously hosted websites on the deep web which are accessible by using specialized software to hide the Internet Protocol (IP) address. IP addresses are assigned to every device that connects to the internet. A Public IP address can be accessed over the internet, a Private IP address cannot be accessed over the internet but are used in internal networks. A Global IP address is specific to a particular network and all devices using that network. Internet Service Providers (ISP) assign Global IP addresses.

The dark web is part of the World Wide Web (WWW) that is only accessible through the use of specialized software (Monk, Mitchell, Frank, & Davies, 2018). The dark web is an encrypted network (to enforce anonymity) that exists predominantly between The Onion Routing (TOR) encryption tools, servers, and their users (Monk et al., 2018). Users of the dark web have the option to remain anonymous and untraceable. Methods employed to access the dark web are quite involved therefore the dark web is not used by the average user. “The globalization of technology and rise of popularity in cryptocurrencies has changed the face of black-market trade and the actors that carry out these crimes” (Paul, 2018, p. 1). Law enforcement agencies and Government Departments are continuously playing catch up in trying to deal with innovations adopted by black market traders to conceal the money trail. “The internet provides an ever-growing number of ways to hide, launder money and pursue a vast range of criminal activities in ways that are difficult to detect or deter” (Slaughter, 2018, p. 118). The handling of criminal activities conducted online is challenging, expensive and requires sufficient quantities of technical resources. The dark web can be used for illegal activities, such as: the sale of drugs (Mackey, 2018; Norbutas, 2018; Porter, 2018), firearms (Porter, 2018), untraceable cryptocurrencies such as Bitcoin (Paul, 2018), child pornography (Dalins et al., 2018), trade in exotic animals (Paul, 2018), sale and purchase of credit card details (Hayes, Cappa, & Cardon, 2018), identify theft (Hayes et al., 2018), money laundering (Dalins et al., 2018; Wegberg, Oerlemans, & Deventer, 2018), amongst others. The monetary cost alone of trying to monitor criminal activities that are conducted online puts a burden on law enforcement agencies and Governments. The Silk Road is a dark net market or an online black market known for the sale of illegal drugs (Dalins et al., 2018; Hayes et al., 2018). It is illegal to use websites that engage with illegal activi-

ties. Due to the ubiquitous nature of the WWW and the anonymity provided, the dark web poses serious challenges to law enforcement agencies around the world. Law enforcement agencies can only achieve so much, members of society must be vigilant and mindful of the legality of the interactions and transactions that they conduct online. It is not only on the deep dark web that illegal activities take place, they are also conducted on the surface web, for example, sale of contraband goods, sale of replicas of branded products, sale of government services with an additional administration charge included, and so forth.

Traditional search engines or web browsers cannot access content available on the dark web. This paper reviews SNS that are accessible through the use of traditional search engines on the surface web where the content is indexed and accessible to standard web browsers. The negative effects of engaging with SNS on the surface web also relate to users engagement with the deep and dark web.

Virtual Private Network (VPN)

VPNs can be used covertly to obscure a users' browsing and online activities from prying eyes. Therefore, illegal activities and transactions can be hidden by using VPN transactions. A Virtual Private Network (VPN) enables the user to send and receive data across a public network, as if it were a private network. A Virtual Private Network (VPN) provides a means of connection to a network within an organisation (as if you were inside the organisation) even though you are not physically present. During the online session the connection is made to the remote network (within the organisation) through the VPN therefore none of the devices (printers, shared disks, and so forth) connected to the local network are available for use to the user as long as the user is remotely connected to the network within the organisation.

Figure 1 illustrates a standard connection to a network within an organisation where there is no need for a Virtual Private Network. The users' remote connection to the network of the business or organisation can be diagrammatically represented as a bubble linked to the target network working within the organization as illustrated in Figure 2.

VPNs' are used legitimately by business users to connect remotely and securely to the companies/ organisations network.

Figure 1. Connection to a network within an organization

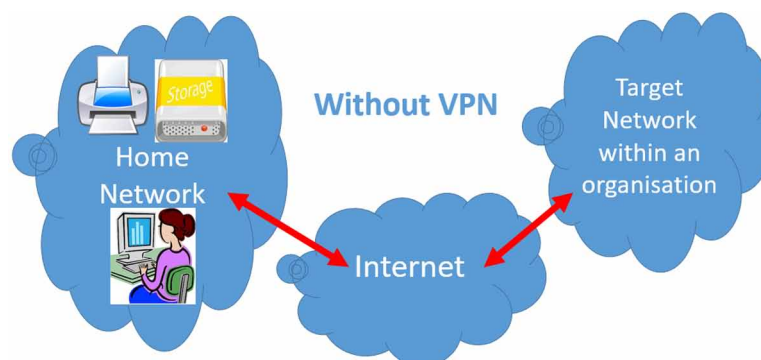
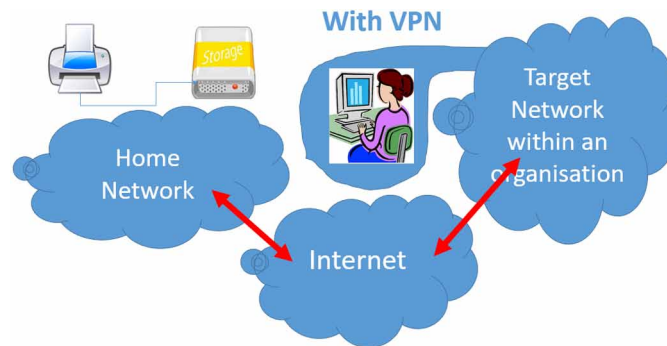


Figure 2. Connection to a network within an organisation using a VPN



THE DARK SIDE OF ENGAGING WITH SOCIAL NETWORKING SITES (SNS)

The massive diffusion of SNS has led to some adverse and undesirable societal consequences (Salo, Mantymaki, & Islam, 2018). SNS both on the surface web and the deep web can have a dark negative side. This chapter focuses on the dark side of engaging with SNS on the surface web. Some of the negative effects include: addiction or addictive behaviour, child pornography, cyberbullying, fake news, Fear Of Missing Out (FOMO), social comparisons, stalking, amongst many others.

Addiction or Addictive Behaviour

“The powerful and addictive sharing functionality of social media presents risks to those who share content and those who consume the content that is shared” (Baccarella et al., 2018, p. 433). Once content is shared through the use of social media, there is no knowing how many people around the world will see, download, or save the content. Shared information, pictures and videos can go viral very quickly, once this content is made publically available there is no way that anyone can delete every instance or trace of the content. In a study conducted by Wang et al. (2018) the findings suggest that addiction to SNS could potentially be a risk factor for the onset of depression in teenagers. The suggestion that addiction to social networking sites could trigger depression in teenagers is a serious issue that deserves further research. Addiction to SNS could also be a risk factor for the onset of depression in adults.

Kanat-Maymon, Almog, Cohen, & Amichai-Hamburger (2018) suggest that the roles of self-esteem and contingent self-worth (CSW) may possibly be associated with excessive and inappropriate use of SNS. It is impossible to know the extent to which users are involved with or subjected to inappropriate use of SNS. In a study conducted by (Atroszko et al., 2018) the findings suggest that “When suggested tentative personality risk factors model were investigated, addictive Facebook use was related to being female, being older, extraverted, narcissistic, having low self-efficacy as well as feeling loneliness and social anxiety” (Atroszko et al., 2018, p. 335). Unfortunately, some users do not realise the negative effects that addictive use of SNS can have on their lives and the lives of others. The findings of Casale & Fioravanti (2018) suggest that there is “a positive association between grandiose narcissism and problematic SNS use” (p. 317). SNS are a recent phenomenon in the history of mankind, further research is needed to ascertain the influence of addictive use of SNS on personal relationships and general well-being.

Excessive use of modern technological devices for social networking can have negative consequences on the following: quality time spent engaging with friends and family (Osatuyi & Turel, 2018), work environment and performance (Moqbel & Kock, 2018; Osatuyi & Turel, 2018), exercising, involvement

with many other activities that are good for both physical and mental welfare, and a reduction in positive emotions (Moqbel & Kock, 2018). “Facebook addiction is related to higher stress, lower general health and lower sleep quality” (Atroszko et al., 2018, p. 335). These negative effects need to be taken seriously and appropriately addressed.

Internet addiction is a recent and changing phenomenon (Mubarak & Quinn, 2017), which has not previously affected society as other addictions have done, therefore, further research is required to promote official recognition of this problem and possibly identify suitable treatments to resolve this problem before social engagement is negatively affected by obsessive use of the internet and SNS. Mubarak & Quinn (2017) suggest that “it is likely that individuals experiencing internet addiction may engage in problem behaviours in cyberspace and create social and psychological problems to other internet users” (p. 9).

Child Pornography

Dalins, Wilson & Carman (2018) suggest that law enforcement agencies show more concern for sites hosting Child Exploitation Materials (CEM) than sites hosting child pornography in the form of cartoons. The sharing of content depicting the exploitation of children for the gratification of others poses a serious challenge to law enforcement agencies. Child pornography and exploitation occurs almost 25% more often than adult pornography (Dalins et al., 2018).

“One site advertised itself as a ‘support’ forum, though in terms of supporting and normalizing paedophilia rather than aiding persons avoid such behavior and actions” (Dalins et al., 2018, p. 71), whilst other sites offered education and training on grooming vulnerable children (Dalins et al., 2018). SNS within the deep and dark web require policing by government supported agencies to infiltrate such sites and monitor the activities of people engaging with these sites.

Cyberbullying

In a study conducted by Mc Hugh, Wisniewski, Rosson, & Carroll (2018) the findings were that “cyberbullying, sexual solicitations, and exposure to explicit content (but not information breaches) can cause symptoms of PTSD” (p. 1182). Post-Traumatic Stress Disorder (PTSD) is a mental health disorder that affects some people who have been exposed to or have personally experienced some horrifying event, or others who have witnessed such events. Experiencing PTSD as a result of engaging with SNS indicates that there is a dark side to SNS. The Health Service Executive (HSE) have provided on their website some helpful advice and who to contact regarding online bullying (HSE, 2018a). “Cyberbullying may be a way to intentionally harm individuals, while oversharing photos of positive experiences unintentionally causes anxiety among those who live lives less glamorous” (Baccarella et al., 2018, p. 432). Some users may not intentionally aim to harm other users by oversharing, not all users will be harmed by the positive posts of others, but some users may through social comparison feel that their lot in life is not as glamorous or successful as others.

Fake News

Fake news is the spreading of untrue facts online or through SNS that may influence readers’ opinions, voting choices, or even, election outcomes. SNS can be used to spread fake news (Baccarella et al., 2018). Users need to be discerning about what they read and what they believe. “Although the actual effect of fake news online on voters’ decisions is still unknown, concerns over the perceived effect of fake news

online have prevailed in the US and other countries” (Jang & Kim, 2018, p. 295). Throughout history there has always been concerns with fake news, alternatively known as propaganda. “The unprecedented popularity of social media for gathering news raises a number of critical questions regarding who trusts news in social media and what sites we trust” (Warner-Soderholm et al., 2018, p. 309). Fake news could have the potential to influence political appointments and could possibly even destroy lives. Some people may not know what or who to believe anymore which may lead to mental stress.

Fear of Missing Out (FOMO)

Fear of Missing Out (FOMO) has the greatest impact on the level of fatigue experienced by users of social media (Bright & Logan, 2018). Lack of sleep can lead to various different mental health disorders. FOMO can have an adverse effect on people’s lives, as an obsession with wanting to keep up with what everyone else is doing, can lead to user fatigue and other adverse consequences. Nicholar Carr (2010) argued the point that people’s attention span has diminished as a result of engaging with the internet and all it offers. “The Shallows: what the internet is doing to our brains” by Nicholar Carr (2010) is an insightful, inspirational, and influential book. After reading this book, one reader selected to “unsubscribe” from numerous e-mail lists, while others deactivated a number of SNS accounts. “The Circle” by Dave Eggers (2013) is another book that would really make the reader consider the amount of information that is shared online, and how all the data mining conducted by organisations is affecting our privacy.

The data mining conducted by some SNS can also affect the privacy of owners and employees of these organisations. Hackers over the years have gained access to information from many organisations around the world proving that there is no way to safely protect one’s privacy. Should an organization which runs a SNS be fined by the European Union for breach of privacy rights, this fine will not bring back the privacy that has been lost to all the users.

Even if an individual is extremely cautious about their own personal information and mindful of every piece of data they share online, others, can upload personal information and images of that person without their explicit permission. This happens all the time and the effort it takes for an individual to get this content taken back down from SNSs is extensive.

In life, it is so easy to go with the flow, without even considering what effects our actions are having on our daily lives and the daily lives of loved ones. It is so easy to get drawn into engaging with online activities, that hours can pass and be lost to the user, which could have been spent engaging with friends, doing productive work, getting exercise, or focusing on things that really matter in life. Some people are so busy recording every meal and experience to post pictures online, that they are not really focusing on the moment, relaxing, and enjoying the time spent with friends. Man has inhabited this earth for years without the need for all this connectivity and lack of privacy. Perhaps one of the reasons obesity and diabetes are on the increase is because mankind now devotes so much time online due to FOMO. If only people would consider what they are missing out by spending so much time online they might then start to relax and enjoy their own life instead of trying to imitate the lives of others as portrayed online.

Social Comparisons

As a result of using SNS some people may get the impression that others posting to the same SNS are leading better lives in comparison to their own. A survey among Korean females found that social comparison was positively associated with the use of blogs, Instagram, and LinkedIn (Chae, 2018). Engagement with SNS can produce social comparison with others (Wang et al., 2018) which may result

in feelings of loneliness in others (Sutcliffe, Binder, & Dunbar, 2018), isolation, anxiety and possibly depression. Online users tend to share the highlights of their lives which may not be representative of the real lives that they are living on a day to day basis. “Those with a high social comparison orientation should limit their use of social media to avoid emotional stress” (Chae, 2018, p. 1663). One’s self esteem can be adversely affected through social comparison with others. As long as people do not realise the potential damage of engaging with SNS they may continue to suffer from social comparisons with others which could lead to mental health issues.

Stalking

Some SNS have the ability to capture a person’s current location through Internet Protocol (IP) address information, this functionality can be used to track or monitor the whereabouts of others (Baccarella et al., 2018). The fact that the location of a person can be tracked may possibly be reassuring to some, for example, parents who have given a mobile phone to a child may then be able to obtain knowledge of their whereabouts at all times. Alternatively, a person’s location may be tracked without their knowledge or permission through the use of technology, by someone who is interested in their whereabouts or someone who holds a grudge, therefore, it is an invasion of personal privacy, ethically unacceptable, and potentially a safety threat. “Studies indicate a strong correlation between high Facebook usage and jealousy in relationships; in other words, as Facebook usage increases, so does jealousy” (Warner-Soderholm et al., 2018, p. 306). Some users may get unrealistic expectations of what life should be like, based on how others portray their lives to be online, this can lead to feelings of jealousy. Some may suffer from negative body image if they compare their body to those of others as they are depicted online. Some images available online may have been photo shopped to make them appear more appealing. Jealousy in relationships can lead to serious mental problems which can only get worse if one continues to stalk others and compare themselves to others as portrayed online.

SOLUTIONS AND RECOMMENDATIONS

The dark side of engaging with SNS will continue to pose problems to society in general as long as people allow SNS to take up too much of their valuable time and influence how they feel about themselves and others. To avoid undue emotional stress, users who are susceptible to a high social comparison orientation should reduce the time spent engaging with SNS (Chae, 2018), or cease to engage with SNS altogether.

Cyberbullying has the potential for serious consequences, for example, someone may feel so bad from being a victim of cyberbullying that they may consider taking their own life by committing suicide (Cohen-Almagor, 2018), or doing something else extreme. “Suicide is a major public health problem and is the second leading cause of death in young people worldwide. Indicating a lack of adequate treatment approaches, recent data suggest a rising suicide rate” (Bailey, Rice, Robinson, Nedeljkovic, & Alvarez-Jimenez, 2018, p. 499). Government funded supports are available, for example a helpline to listen to victims and help them to deal effectively with the problem (HSE, 2018a, 2018b). Unfortunately, not all victims of online bullying are aware of these services. People of all ages can be victims of cyberbullying and government provided supports should be available to help and guide all victims about the best ways to deal with the online persecution.

SNS can be used to advertise and sell all sorts of goods, including drugs and other illegal products. Concerted efforts by law enforcement agencies, the public, public health authorities, government ad-

ministrators, and technology companies will be required to successfully combat the sale of illegal drugs online (Mackey, 2018). Due to the complexities involved in dealing with cybercrimes “too few appear currently willing or able to grapple with the issues, let alone provide satisfying answers” (Slaughter, 2018, p. 118). Further research is required to determine the most productive and cost effective methods to combat cybercrimes.

Organisations’ should leverage their information security policies based on the perceived threats and benefits of employees engaging with SNS (Silic & Back, 2016). Should an employee be addicted to engaging with SNS and possibly engage during working hours, then the work that they are supposed to be doing may be neglected. Organisations’ should be aware of the perceived threats and benefits of SNS, so that they can effectively deal with these by taking appropriate action. “Fake news is a critical major issue that social networking websites can ameliorate with vigilance and skillful use of technology” (Morales, Sosa-Fey, & Farias, 2017, p. 87). Fake news poses a real challenge to society and requires further investigation.

FUTURE RESEARCH DIRECTIONS

Further research is required to determine the most productive and cost effective methods to combat cybercrimes. Law enforcement agencies and Governments have numerous challenges ahead in dealing with the dark side of SNS and cybercrime on the surface web. This is only scratching the surface as the deep and dark web are more embedded in areas where users want to hide their identity, therefore, it is much more difficult to trace the online actions of users.

Fake news has the potential to influence politics and also to destroy lives. Fake news poses a real challenge to society and requires further investigation. Members of society deserve to know the truth so that they can make informed decisions based on honest facts.

The suggestion that addiction to SNS could trigger depression in teenagers is a serious issue that deserves further research. Internet addiction is a recent and changing phenomenon (Mubarak & Quinn, 2017), which has not previously impacted on society as other addictions have done, therefore, further research is required to promote official recognition of this problem. SNS are a recent phenomenon in the history of mankind, further research is needed to ascertain the influence of addictive use of SNS on personal relationships and general well-being.

CONCLUSION

Although SNS are used by many people all around the world to connect with loved ones and friends in a positive context, alas, SNS are also used by many people in a negative context, including some of the topics discussed in this chapter. There are some dark sides or negative aspects to human engagement with SNS which may include the following: exposure to possible risks, spending too much time online, deleterious impacts, access to black market traders, untraceable cryptocurrencies, sale of drugs and firearms, child pornography, trade in exotic animals, identity theft, and money laundering.

Some concerns with users’ engagement with SNS are as follows: images going viral, internet addiction, depression in teenagers, lack of quality time to spend with friends and family, impact on work performance, physical and mental welfare, higher stress levels, lack of sleep, loneliness, isolation, anxiety, and jealousy, amongst many others.

These negative effects need to be taken seriously and appropriately addressed. Users should be encouraged to question the short and long term risks of engaging with SNS. Users of Social Networking Sites within the surface web and the deep and dark web require the support of government agencies in dealing with the inappropriate activities of other people engaging with these sites. The monetary cost of dealing with cybercrime puts a burden on Law Enforcement Agencies and Governments.

Society as a whole needs to consciously consider all of the negative effects of engagement with SNS, discuss these with friends, family, and work colleagues then try to reach a consensus on how best to address all of these issues.

REFERENCES

- Atroszko, P., Balcerowska, J., Bereznowski, P., Biernatowska, A., Pallesen, S., & Andressen, C. (2018). Facebook addiction among Polish undergraduate students: Validity of measurement and relationship with personality and well-being. *Computers in Human Behavior*, 85, 329–338. doi:10.1016/j.chb.2018.04.001
- Baccarella, C., Wagner, T., Kietzmann, J., & McCarthy, I. (2018). Social media? It's serious! Understanding the dark side of social media. *European Management Journal*, 36(4), 431–438. doi:10.1016/j.emj.2018.07.002
- Bailey, E., Rice, S., Robinson, J., Nedeljkovic, M., & Alvarez-Jimenez, M. (2018). Theoretical and empirical foundations of a novel online social networking intervention for youth suicide prevention: A conceptual review. *Journal of Affective Disorders*, 238, 499–505. doi:10.1016/j.jad.2018.06.028 PMID:29936387
- Bright, L., & Logan, K. (2018). Is my fear of missing out (FOMO) causing fatigue? Advertising, social media fatigue, and the implications for consumers and brands. *Internet Research*, 28(5), 1213–1227. doi:10.1108/IntR-03-2017-0112
- Carr, N. (2010). *The Shallows: what the internet is doing to our brains*. New York, NY: W. W. Norton & Company.
- Casale, S., & Fioravanti, G. (2018). Why narcissists are at risk for developing Facebook addiction: The need to be admired and the need to belong. *Addictive Behaviors*, 76, 312–318. doi:10.1016/j.ad-beh.2017.08.038 PMID:28889060
- Chae, J. (2018). Reexamining the relationship between social media and happiness: The effect of various social media platforms on reconceptualized happiness. *Telematics and Informatics*, 35(6), 1656–1664. doi:10.1016/j.tele.2018.04.011
- Cohen-Almagor, R. (2018). Social responsibility on the Internet: Addressing the challenge of cyberbullying. *Aggression and Violent Behavior*, 39, 42–52. doi:10.1016/j.avb.2018.01.001
- Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation*, 24, 62–71. doi:10.1016/j.diin.2017.12.003
- Eggers, D. (2013). *The Circle*. McSweeney's Books.
- Eiriraki, M., Gao, J., Varlamis, I., & Tserpes, K. (2018). Recommender systems for large-scale social networks: A review of challenges and solutions. *Future Generation Computer Systems*, 78, 413–418. doi:10.1016/j.future.2017.09.015

Facebook. (2018). *Connect with friends and the world around you on Facebook*. Retrieved from <https://www.facebook.com/>

Firefox. (2019). *Mozilla Firefox*. Retrieved from <https://www.mozilla.org/en-US/firefox/new/>

Flickr. (2018). *Flickr at its best is a place to connect, to discover, and to evolve as photographers and lovers of photography*. Retrieved from <https://www.flickr.com/>

Google+. (2018). *Collections*. Retrieved from <https://plus.google.com/discover>

Google. (2019). *Google Chrome*. Retrieved from https://www.google.com/chrome/?brand=CHBD&gclid=EAIaIQobChMI1L2JsqmB4AIVqrXtCh226QumEAAYASAAEgLzZvD_BwE&gclsrc=aw.ds

Grindr. (2018). *The World's largest social networking app for gay, bi, trans, and queer people*. Retrieved from <https://www.grindr.com/>

Guinta, M., & John, R. (2018). Social media and adolescent health. *Pediatric Nursing*, 44, 196–201.

Hayes, D., Cappa, F., & Cardon, J. (2018). A framework for more effective dark web marketplace investigations. *Information*, 9(186), 1–17.

HSE. (2018a). *Bullying and harassment Bullying can affect anyone. It isn't always easy to deal with a bully, no matter your age*. Retrieved from https://www2.hse.ie/wellbeing/mental-health/bullying-and-harassment.html?gclid=EAIaIQobChMIoaX58ZfA4QIVz53tCh1GSQDPEAAYASAAEgLU7fD_BwE&gclsrc=aw.ds

HSE. (2018b). *Cyberbullying is a new form of bullying, but it can be even more harmful than one might think*. Retrieved from <https://www2.hse.ie/wellbeing/mental-health/cyberbullying.html>

Instagram. (2018). *Sign up to see photos and videos from your friends*. Retrieved from <https://www.instagram.com/>

Jang, S., & Kim, J. (2018). Third person effects of fake news: Fake news regulation and media literacy interventions. *Computers in Human Behavior*, 80, 295–302. doi:10.1016/j.chb.2017.11.034

Kanat-Maymon, Y., Almog, L., Cohen, R., & Amichai-Hamburger, Y. (2018). Contingent self-worth and Facebook addiction. *Computers in Human Behavior*, 88, 227–235. doi:10.1016/j.chb.2018.07.011

LinkedIn. (2018). *Your dream job is closer than you think*. Retrieved from <https://www.linkedin.com>

Liu, F., & Lee, H. (2010). Use of social network information to enhance collaborative filtering performance. *Expert Systems with Applications*, 37(7), 4772–4778. doi:10.1016/j.eswa.2009.12.061

Mackey, T. (2018). Opioids and the Internet: Convergence of technology and policy to address the illicit online sales of opioids. *Health Services Insights*, 11, 1–6. doi:10.1177/1178632918800995 PMID:30245569

McHugh, B., Wisniewski, P., Rosson, M., & Carroll, J. (2018). When social media traumatizes teens: The roles of online risk exposure, coping, and post-traumatic stress. *Internet Research*, 28(5), 1169–1188. doi:10.1108/IntR-02-2017-0077

Microsoft. (2019). *Windows Internet Explorer*. Retrieved from <https://www.microsoft.com/en-us/download/internet-explorer.aspx>

- Monk, B., Mitchell, J., Frank, R., & Davies, G. (2018). Uncovering Tor: An examination of the network structure. *Security and Communication Networks*, 2018, 1–12. doi:10.1155/2018/4231326
- Moqbel, M., & Kock, N. (2018). Unveiling the dark side of social networking sites: Personal and work-related consequences of social networking site addiction. *Information & Management*, 55(1), 109–119. doi:10.1016/j.im.2017.05.001
- Morales, K., Sosa-Fey, J., & Farias, J. (2017). Social Media: Are the benefits worth the risks for business? *International Journal of Business and Public Administration*, 14(1), 87–97.
- Mubarak, A., & Quinn, S. (2017). General strain theory of Internet addiction and deviant behaviour in social networking sites (SNS). *Journal of Information, Communication and Ethics in Society*. doi:10.1108/JICES-08-2016-0024
- Norbutas, L. (2018). Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. *The International Journal on Drug Policy*, 56, 92–100. doi:10.1016/j.drugpo.2018.03.016 PMID:29621742
- Osatuyi, B., & Turel, O. (2018). Tug of war between social self-regulation and habit: Explaining the experience of momentary social media addiction symptoms. *Computers in Human Behavior*, 85, 95–105. doi:10.1016/j.chb.2018.03.037
- Paul, K. (2018). Ancient artifacts vs. digital artifacts: New tools for unmasking the sale of illicit antiquities on the Dark Web. *Arts*, 7(12), 1–19.
- Pinterest. (2018). *Pinterest helps you find ideas to try*. Retrieved from <https://www.pinterest.ie/>
- Porter, K. (2018). Analyzing the DarkNetMarkets subreddit for evolutions of tools and trends using LDA topic modeling. *Digital Investigation*, 26, S87–S97. doi:10.1016/j.diin.2018.04.023
- QZone. (2018). Retrieved from <https://qzone.qq.com/>
- Reddit. (2018). *Reddit: the front page of the internet*. Retrieved from <https://www.reddit.com/>
- Salo, J., Mantymaki, M., & Islam, A. (2018). The dark side of social media - and Fifty Shades of Grey introduction to the special issue: The dark side of social media. *Internet Research*, 28(5), 1166–1168. doi:10.1108/IntR-10-2018-442
- Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior*, 60, 35–43. doi:10.1016/j.chb.2016.02.050
- Skype. (2018). *Skype makes it easy to stay in touch*. Retrieved from <https://www.skype.com>
- Slaughter, R. (2018). The IT revolution reassessed part one: Literature review and key issues. *Futures*, 96, 115–123. doi:10.1016/j.futures.2017.12.006
- Snapchat. (2018). *A new way to look*. Retrieved from <https://www.snapchat.com/>
- Sutcliffe, A., Binder, J., & Dunbar, R. (2018). Activity in social media and intimacy in social relationships. *Computers in Human Behavior*, 85, 227–235. doi:10.1016/j.chb.2018.03.050
- Tinder. (2018). *Match. Chat. Date*. Retrieved from <https://tinder.com>

Tumblr. (2018). Come for what you love. Stay for what you discover. Retrieved from <https://www.tumblr.com/>

Twitter. (2018). *See what's happening in the world right now*. Retrieved from <https://twitter.com>

Viber. (2018). *Free and secure calls and messages to anyone, anywhere*. Retrieved from <https://www.viber.com/>

Wang, P., Wang, X., Wu, Y., Xie, X., Wang, X., Zhao, F., ... Lei, L. (2018). Social networking sites addiction and adolescent depression: A moderated mediation model of rumination and self-esteem. *Personality and Individual Differences*, 127, 162–167. doi:10.1016/j.paid.2018.02.008

Warner-Soderholm, G., Bertsch, A., Sawe, E., Lee, D., Wolfe, T., Meyer, J., ... Fatilua, U. (2018). Who trusts social media? *Computers in Human Behavior*, 81, 303–315. doi:10.1016/j.chb.2017.12.026

Wegberg, R., Oerlemans, J., & Deventer, O. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419–435.

WhatsApp. (2018). *Simple. Secure. Reliable messaging*. Retrieved from <https://www.whatsapp.com/>

YouTube. (2018). *Best of YouTube*. Retrieved from <https://www.youtube.com/>

ADDITIONAL READING

Ampong, G., Mensah, A., Adu, A., Addae, J., Omoregie, O., & Ofori, K. (2018). Examining self-disclosure on social networking sites: A flow theory and privacy perspective. *Behavioral Science*, 8(58), 1–17. PMID:29882801

Errasti, J., Amigo, I., & Villadangos, M. (2017). Emotional uses of Facebook and Twitter: Its relation with empathy, narcissism, and self-esteem in adolescence. *Psychological Reports*, 120(6), 997–1018. doi:10.1177/0033294117713496

Fox, J., & Moreland, J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior*, 45, 168–176. doi:10.1016/j.chb.2014.11.083

Parks, R., Lowry, P., Wigand, R., Agarwal, N., & Williams, T. (2018). Why students engage in cyber-cheating through a collective movement: A case of deviance and collusion. *Computers & Education*, 125, 308–326. doi:10.1016/j.compedu.2018.04.003

Quach, S., & Thaichon, P. (2018). Dark motives-counterfeit selling framework: An investigate on the supply side of the non-deceptive market. *Marketing Intelligence & Planning*, 36(2), 245–259. doi:10.1108/MIP-04-2017-0069

Sapountzi, A., & Psannis, K. (2018). Social networking data analysis tools & challenges. *Future Generation Computer Systems*, 86, 893–913. doi:10.1016/j.future.2016.10.019

Topaloglu, M., Caldibi, E., & Oge, G. (2016). The scale for the individual and social impact of students' social network use: The validity and reliability studies. *Computers in Human Behavior*, 61, 350–356. doi:10.1016/j.chb.2016.03.036

Zhang, X., Shan, L., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management*, 55(4), 482–493. doi:10.1016/j.im.2017.11.003

KEY TERMS AND DEFINITIONS

Addiction or Addictive Behaviour: Actions which a person can no longer control. Someone may go online to send an e-mail, get distracted and remain online for several hours, and possibly forget to send the e-mail.

Child Pornography: Online sharing of content which shows the sexual exploitation of children.

Cyberbullying: A form of bullying that occurs online.

Dark Web: The dark web refers to a number of anonymously hosted websites on the deep web which are accessible by using specialized software to hide the internet protocol (IP) address.

Fear of Missing Out (FOMO): Some people are afraid to go offline in case they miss out on some exciting piece of news.

Fake News: The spreading of untrue facts online or through Social Networking Sites that may influence readers' opinions, voting choices, and election outcomes.

IP Address: IP addresses are assigned to every device that connects to the internet.

Social Comparisons: As a result of using social networking sites some people may get the impression that other users are leading better lives in comparison to their own.

Social Networking Sites: Social networking sites (SNS) enable users to interact with other people online; similar to how people may socially interact offline by sharing personal experiences, images, making plans, and so forth.

Stalking: A person's location may be tracked without their knowledge or permission through the use of technology, by someone who is interested in their whereabouts or someone who holds a grudge; therefore, it is an invasion of personal privacy, ethically unacceptable, and potentially a safety threat.

Virtual Private Network (VPN): A virtual private network (VPN) provides a means of connecting to a network within an organisation (as if you were inside the organisation) even though you are not physically present.

Cyberstalking: The New Threat on the Internet

Edith Huber

 <https://orcid.org/0000-0003-3373-0870>

Danube University Krems, Austria

Roman H. Brandtweiner

Vienna University of Economics and Business, Austria

INTRODUCTION

The phenomenon of stalking itself is as old as humankind itself. The past years and the expansion of digitalization have put the crime of stalking in a new light. A representative study from the USA, shows that one in four Americans has already been “harassed” online. (Duggan, 2017) If stalking in the traditional sense (also known as offline stalking or classic stalking) is described as obsessive harassment / threat over a longer period, it takes on a new criminal dimension as soon as connected communication takes place. New forms of crime such as cyberstalking, cyberbullying, and romance scams have now reached our everyday lives. The main objective of this article is to introduce a representative study on cyberstalking cases in Austria to the scientific community. In addition, it should provide a clearer picture of cyberstalking based on evidence-based international data.

BACKGROUND

There is no doubt that stalking is a common criminal offence that has taken on a new dimension with the expansion of the Internet. According to Pathe and Mullen (Pathe & Mullen, 1997), stalking is described as a set of behaviours in which the stalker continuously and violently penetrates the victim’s privacy and harasses the victim through personal contacts or the use of communication media. (Pathe & Mullen, 1997) Cyberstalking is often viewed as a natural continuation of offline stalking given their conceptual and operational overlap. In classical stalking one speaks of persistent persecution. This includes persecution, ambush, trespassing, and the unintentional receipt of gifts, letters and telephone calls. The development of telecommunications has brought about a change in the way the media communicate, with the result that traditional communication methods have been replaced by Internet communication.

This led to the development of new stalking methods, which found their way into encyclopaedias under the neologism of “cyberstalking”. Hoffmann defines cyberstalking as “the obsessive persecution or harassment of another person using the Internet, e-mail, an intranet or related electronic media”. (Hoffmann, 2006, p 197) The US government defines cyberstalking as “the use of the Internet, email, or other electronic communications devices to stalk another person”. (US Attorney General, 1999) In summary, ‘cyberstalking’ means stalking processes that occur with the help of new electronic communication devices, i.e. mobile phones, smartphones, laptops or other networked mobile devices. With these devices, chatting, sharing pictures and videos or transmitting voice recordings is made much easier

DOI: 10.4018/978-1-5225-9715-5.ch043

individually and in communities. The permanent availability of the service programs on these devices makes it possible to communicate at any time of the day or night, as well as anywhere else.

The most common definitions of cyberstalking can be found in legal literature. Therefore, this definitions are bound to the legislation of the respective country and can therefore hardly provide a complete overview of all facets of cyberstalking. For a pure legal assessment, it is not necessary to cover the social phenomenon cyberstalking in all its facets. Laws have the function of subsuming accurate facts of life under legal regulations and deducing legal consequences from them. We will not stick to country bound legal definitions of cyberstalking. We see it as a recent social phenomenon, which is bound to electronic communication. If we see cyberstalking primarily as abusive communicative behaviour, we can follow Forgó et al. (Forgo, 2010) and define the term cyberstalking (in narrower sense) not only as threats and coercion but also as actions, which, due to their continuity and duration, lead to an unreasonable impairment of lifestyle. In a broader sense, the term cyberstalking includes also attacks on computer systems and defamatory publications on websites, in online forums, or in social networks, but also unwelcome publication of photos. (Forgo, 2010)

These are typical classifications from classical stalking research. According to Goodno (Goodno, 2007), five factors differentiate cyberstalking from traditional stalking. First, the perpetrators who use cyberstalking as a method are much more efficient than classical delinquents are. Due to the characteristics of internet communication, the victim is immediately and more widespread harassed than in traditional stalking. Secondly, there is no physical presence required to engage in cyberstalking. Third, cyberstalkers usually remain anonymous. By combining second and third, it is therefore much easier to engage in cyberstalking. This makes it easier for cyberstalkers to assign the harassment / threat to third parties. (Goodno, 2007) Bocij (Bocij, 2006), on the other hand, assumes that cyberstalking can also lead to physical violence in a later episode. (Bocij, 2006) Whether a person perceives cyberstalking as a threat / harassment also depends on the personal sensitivity of the victim. Some people feel because of certain actions as victims some do not. If a certain behaviour is considered as cyberstalking from a legal point of view, the person who is the victim must not necessarily feel himself / herself as a stalking victim. (Huber, 2012) Therefore, cyberstalking as a social phenomenon can only be understood by applying the current social norm. The social convention under which information is communicated and shared is an important premise whether an action is regarded as cyberstalking or not. (Nissenbaum, 2004)

Who Are the Perpetrators?

Example: Jason is not happy in his job. All the suggestions he makes to his boss are ignored. Then he also receives a letter of termination. Angry and disappointed, he wants to take revenge on his boss. He spreads lies about his boss on various internet platforms such as LinkedIn and Facebook.

The scientific literature in the field of stalking and cyberstalking focuses very strongly on the psychological condition of the perpetrators. This is due to the fact that most of the studies were conducted in the clinical field, where mentally ill stalkers were examined or the data about the perpetrators were collected through victim interviews. (Mullen & Pathe, 2000) However, if we take a more detailed look at the term “perpetrator”, it has to be said that we can only speak of a “perpetrator” in a legal sense when the person in question was sentenced by a court of law. Up to this point, we should call them suspects or strong suspects. The literature distinguishes five different types of perpetrators from classical stalking research: 1. The rejected stalker: often they are former partners of the victim. Violent acts are common in this type of stalker. In addition, personality disorders are often diagnosed. 2. The intimacy seeker: the typical cases of “erotomania” fall under this category. A typical example of this is that the stalker is often

in love with a celebrity. Violent actions rarely occur. 3. The social incompetent: this type of stalker often does not understand or misinterpret the victim's rejection due to lack of social skills. In many cases, the stalker is less intelligent or has social deficits. Violent actions are rare. 4. The revenge addict: this type of stalker feels misunderstood and goes on a personal revenge campaign, e.g. against a former boss. A paranoid clinical picture is a conspicuous component. 5. Sexual delinquents: In these cases, stalking is often the preliminary stage to a sexual offence. Often there is a predisposition and previous convictions. (Mullen PE, Pathe M, 2000) Bocij noted that cyberstalking offenders very often seek allies to stalk the victim together. He distinguishes three levels of computer education among the victims: novice, intermediate and expert. It was found that newcomers feel more threatened than experts do. On the other hand, the experts found more attacks on their PCs than people with average computer skills did. This suggests a connection between computer skills and cyberstalking behaviour. (Paul & Leroy, 2002) In another study by (Storey, J.E. & Hart, S.D., 2011), a stalker profile (not only the cyberstalker profile) was examined in Canada. Most of the perpetrators were male ($n=29$, 91%). The median age was 42 years and the most were single. Only 13,41% were unemployed and had a history of treatment for mental health problems ($n=10$, 31%). The literature knows different clinical patterns about stalking perpetrators. by (Storey, J.E. & Hart, S.D., 2011). At the psychopathological level of this multi-axial classification, 3 categories are distinguished: 1. psychotic stalkers, 2. progressive psychopathological development, and 3. Stalkers without relevant psychiatric disorder. (Dressing, H. & Foerster 2010) drivers for cyberstalking are different to the ones just discussed for classical stalking. Tokunaga, R. S., & Aune, K. S. summarize the following four motives. (Tokunaga, R. S., & Aune, K. S. 2017). 1) Hyperintimacy involves messages delivered electronically or digitally in relentless pursuit of a relationship. (Spitzberg & Hoobler, 2002). Hyperintimate messages are generally harmless but nonetheless considered as a form of harassment. 2) Threat messages in online relational pursuit involve implicit or explicit claims of bringing harm to the victim. Threats of harm can range from damaging one's reputation to more sinister acts of bodily injury. (Spitzberg & Hoobler, 2002) 3) Sabotage entails compromising targeted person's reputations by publishing either true or fabricated information about her or him. (Spitzberg & Hoobler, 2002). Typical examples are the spreading of rumors or gossip to people close to the victim. Cyberstalkers often sabotage the public image or videos of the social or professional lives of their victims. 4) Invasion is considered the most menacing set of cyberstalking behaviors because it involves many actions that profoundly interfere with the targets' livelihoods. Activities attributed to invasion can go as far as property damage and identity theft. (Spitzberg & Hoobler, 2002). Information theft and surveillance are two main types of invasion behaviors. Cyberstalkers sometimes attempt to find out and succeed in gathering private information about their victims using various means of communication technology (Bocij, 2006) (Tokunaga, R. S., & Aune, K. S. 2017)

One can say that there is no single definition of cyberstalking. This is always dependent on the legal, technical, cultural and social framework. This also results in conceptual overlaps with other phenomena such as cyberbullying, hate postings, other revenge crimes or other forms of communicative violence on the Internet. Nevertheless, the discussion about cyberstalking is more topical than ever. New challenges are emerging in sociology, justice, the police, psychology and cyber security.

In the next chapter, we will investigate further characteristics of cyberstalking offenders, based on a content analysis of court files. However, these approaches still need to be verified in the future at cyberstalking perpetrators. Now, however, there is no scientific evidence to show whether the clinical pictures of the classic stalker correspond to those of the cyberstalker. Taking a closer look to cyberstalking one of the most important questions is whether perpetrators, victims and the typical courses of events (*modus operandi*) are identical.

FOCUS OF THE ARTICLE

3

Bright Field - Dark Field

In crime, we distinguish between bright field and dark field numbers. The bright field number describes the amount of delicts that are known to the public sector as an “official” criminal offence. The dark-field-number, on the other hand, is the estimated number of unreported / undetected cases. The description of bright field and dark field data is fundamentally dependent on the respective legal and cultural situation of the country and on the methods of measurement. (Huber, 2019) In many countries, cyberstalking is not a criminal offence of its own, but is labelled as “dangerous threat / harassment” or “Cybercrime”. In methodological terms, it is always a challenge to collect the dark figures of crime. This requires a large number of long and cross-sectional studies, which are lacking for all cybercrime in general and for cyberstalking in specific. The article focusses on the phenomenon of cyberstalking solely using evidence-based data. The authors avoid the exclusive reflection in connection with classical stalking and other methodological weaknesses found in numerous studies like the limitation of the target groups, which distorts the representativeness of the results. Most studies on this or related topics are not representative, or do not exactly define the concept of cyberstalking. For example, there is a representative study on cyberbullying behaviour in the D-A-CH region (Germany, Austria, and Switzerland). (Schneider, C.; Leest, 2018) Similar to Huber’s study, this survey shows that about one third of all respondents were victims of cyberbullying. This raises the question of the extent to which individual persons can distinguish the term cyberstalking from cyberbullying. “Cyberbullying is the deliberate insulting, threatening, exposing or harassing of others with the help of Internet and mobile phone services over a longer period of time. The perpetrator - also known as a “bully” - looks for a victim who cannot or only with difficulty defend himself against the attacks. There is thus an imbalance of power between perpetrator and victim, which the perpetrator exploits, while the victim is socially isolated” (Klicksafe.de, 2018) The demarcation from cyberstalking is not easy in this case, because cyberbullying methods can also be components of cyberstalking. The difference is in long lasting, obsessive threat or harassment that affects lifestyle.

In the year 2009, Huber conducted a representative study in Austria. The aim of this research was to provide a detailed documentation and description of the cyberstalking field in Austria. This survey was the first research project that delivered reliable information on detected as well as on unreported cases. (Huber, 2012) In the process, n=747 persons aged between 18 and 66 were interviewed throughout Austria. At this time (2009), around 83% of all men and 77% of all women in Austria were online (INTEGRAL, 2010). Only for comparison currently (2018), 92% of the Austrian males and 80% of the Austrian females have internet access. (INTEGRAL, 2018) Despite of the general expansion of Internet usage, there is still a clear difference between the genders. This means that a gender gap is constantly present. Factors such as gender, income, age and education are still variables of the ‘digital divide’. In the study quoted above, the people were asked whether they have ever been stalked in their lives. In particular, stalking methods via e-mail, SMS, chat and websites - platforms such as Facebook - were in the focus of the survey. Messenger services such as WhatsApp, Snap Chat etc. were not in use in Austria at this time and therefore have not been included in the questionnaire. In this context, 34% felt harassed / threatened by e-mail stalking, 17% by SMS stalking, 6% by chat stalking and only 3% by cyberstalking on websites and platforms. This figures show that more than a third of the population has already had cyberstalking experience. Another interesting factor in this study of the unreported cases is that around 48% of the surveyed men said they had already become victims of stalking. This number differs massively from the number of reported cases. The reason for this lies in the different behaviour to take a

criminal charge between men and women. Significantly, fewer men are willing to report a cyberstalking or stalking action than women. (Huber, 2012)

Unfortunately, there are no similar representative studies on this topic to provide a global overview of the dark field. In general, we can conclude that the number of unreported cases is much higher than the number of reported cases. This difference results from various factors. On the one hand, not all cyberstalking victims report the crime. Even if the crime is reported, the deeds occur in combination with other crimes such as cybercrimes, domestic violence, harassment or dangerous threats. On the other hand, there is no clear distinction of terms worldwide, so that different cyber violent crimes, such as cyberbullying, online violence or hate postings, are often used as synonyms.

Case Study: Analysis of Court Files in Vienna (Huber & Pospisil, 2017)

As part of a research project in Vienna, a file analysis of cybercrime offences from 2006 to 2016 was carried out at the Vienna Criminal Court (Straflandesgericht Wien). The reason for the selection of the investigation period was that from 2006 onwards cybercrime cases were counted separately in the Austrian criminal statistics. Cybercrimes in its narrower meaning as well as cybercrimes in the broader sense were analysed. Based on that from 2006 ongoing distinction between traditional crime and cybercrime, around 5,408 files were available to the public prosecutor's office and the court in Vienna. A central research goal of the study was the development of reliable offender profiles and victim profiles. A sample of $n=20\%$ was drawn from $N=5,408$ court files. A quantitative document analysis according to Döllinger (Döllinger, 1984) was used as a research method for the analysis of the files. For this purpose, an analysis sheet, which contained all interesting variables, was developed. After collecting the data, a statistical analysis was executed. SPSS was used for the data analysis. Both univariate, bivariate and multivariate analysis methods were used to show the frequencies, correlations and prediction probabilities of the variables. Furthermore, cluster analysis and logistic regression were employed during the analysis process. One of the main results of the study was a catalogue of different offender profiles of cyber criminals. Based on a cluster analysis, a typologisation of cyber criminals was developed. Demographic characteristics were used as distinctive variables. The average cluster quality is 0.4, so the model is of mediocre quality. The gender variable, at 100%, was most strongly included in type formation. This is also the reason why the description of offender types is assigned to specific genders. This is followed by the education variable (52%) and the employment variable (35%). The variable age was the least taken into account in type formation (10%). Two clearly distinguishable offender types could be identified.

If we now look at the results regarding an "ideal type" in the statistical sense (more than 50%), the typical cyberstalking-defendants suspect looks like this: More than half of the suspects are male. People of this type have a low level of education. Some do not have any vocational training and have only completed primary school. Many do not have a regular job. The average age is 29.91 years (arithmetic mean). Apart of the average age of 29.91, a large part of young people up to 20 years (80%) fall into this group. In this group, most suspects have a criminal record (57%). Even though the number of cases on the problematic background is small, it should be mentioned that 64% of all persons with difficult family circumstances and 68% of all persons with addictive behaviour are of this type. An interesting feature of this type is that the suspects have no special computer skills. Their IT skills are primarily self-taught and they have good user skills.

The second type, in which cyberstalking offences have also occurred, is the group of women. The group comprises 18%. This means that about one fifth of the suspects are female. This also corresponds to the common criminal analysis of other criminal offences. The educational status is relatively differ-

ent. While half of the persons (50%) have a low level of education, a further 44% have a school-leaving certificate level. Only 6% have a high level of education. The majority of people of this type are not in regular employment, only 19% are in regular employment. This can be explained by the fact that categories such as ‘maternity leave’ or ‘pension’ can be found here. Persons of this type are on average around 32 years old (arithmetic mean). Suspects of this type are highly likely (69%) to have no criminal record and are usually not remanded in custody (81%). Women committed most of the crime (56%) as individual perpetrators. If one looks at the motives of cyberstalking suspects, it can be said that in almost all cases there was a relationship between perpetrator and victim. (Huber & Pospisil, 2017) This can be a former love relationship or an acquaintance relationship. The main motive is always revenge on a particular person.

The Unknown Perpetrator

Most delinquents therefore have a personal motive for the crime. Recent findings show us that cyberstalking is also committed by offenders who are unknown to the victims.

A current real life example of an “unknown offender” from Austria shows the following cause of events: An IT consultant, male, 55-year-old let a woman die, not really just virtually. The offender, who knew his neighbour only fleetingly, had chosen her as his victim randomly. His first action was, creating a faked Facebook profile of the woman where she offered sexual services on a professional base. The peak of the stalking activities were reached when the stalker posted a forged death certificate of the woman and reported his victim to energy suppliers and her telephone company as dead by sending e-mails to these companies pretending to be a relative. On a mourning website, the stalker published an obituary with a photo of the allegedly deceased. (n. A., 2018)

Resourceful IT-savvy people try to threaten their victims with false identities on the Internet. This pattern is often found in personal revenge or lust motifs. There does not necessarily have to be a close personal relationship or any relationship at all between perpetrator and victim. The perpetrators are IT-savvy and have the knowledge to camouflage themselves. Encryption techniques are often used to conceal the identity of the perpetrator.

Bocij (Bocij, 2006) already speaks in 2006 of the fact that there are resourceful cyber criminals who smell a business model in the field of Internet stalking and offer their services via the dark web. Current analyses by Europol (Europol, 2018) show that a new extortion method (Romance-Scams) has developed which can be considered as a version of cyberstalking. The criminal’s motives are extrinsic. They have their origin in external stimuli; their own actions are seen as building blocks for the achievement of an external goal, such as earning money. (McClelland, 1987) In such a situation, there is no connection between perpetrator and victim normally. These perpetrators also often act in groups and mask their actions.

Who Are Victims?

Example: 22-year-old Susan is separating from her boyfriend Peter. He cannot cope with the breakup. After the initial sadness about the loss, Peter becomes more and more angry. He wants to take revenge on Susan. In his revenge plans, he wants to inflict special damage and so he decides to disturb Susan’s digital life. Since Susan and Peter had a common PC, he knows the login information of Susan’s social media platforms and e-mail accounts. In no time, he has changed all their passwords so that Susan has no access to her e-mails or social media accounts. He now uses her accounts and posts obscene images of her.

When the phenomenon of stalking began to be addressed at the beginning of the 1990s, it was assumed that the stalking problem almost exclusively affected prominent people, such as Hollywood stars. Shortly afterwards, stalking victims were also discovered among the average population. (Dressing, Kuehner, & Gass, 2005) Stalking itself is a worldwide phenomenon and occurs in all cultural contexts. The spread of cyberstalking, on the other hand, depends on digitisation and broadband rollout in the respective countries. Various studies have shown that in cases of offline stalking, mainly women are the victims (90%). Numerous researches have shown that most women are victims of domestic violence in combination with stalking. (Dressing, Kühner, & Gass, 2007) (Mullen & Pathe, 2000) (McFarlane & Bocij, 2003) However, the question is, is it different with cyberstalking victims? If one analyses the victimization of cyberstalking, one is confronted relatively quickly with the problem that the person concerned has to prove (in a legal sense) that she/he has become a victim. If one orients oneself towards the traditional concept of stalking, the victim must prove that he or she has been harassed or threatened over a longer period of time, so that his or her lifestyle has been impaired. (Huber, 2012) Unfortunately, the psychological component is often ignored in this definition. The fact whether someone sees themselves as cyberstalking victims depends on the personal attitude of the victims. Some people do not mind receiving 70 WhatsApp messages a day. Others feel harassed or threatened by three messages. Referring to the above mentioned file analysis at the Vienna Criminal Court; no significant differences could be identified among the cyberstalking victims. However, one can tend to say that if the perpetrator and the victim were previously in a love relationship, there is a greater probability that the victim is a woman. On statistical average, women and men are equally likely to become victims of cyberstalking (Huber & Pospisil, 2017) As technology develops, cyberstalking victims become older. While the average cyberstalking victim in 2009 was around 35 years old (Huber, 2012), there are now younger and older victims. Bocij interviewed 169 Internet users about cyberstalking behaviour. He concentrated on the experiences of the victims. (Perpetrators themselves were not interviewed.) Over 80% had already had experience with cyberstalking, 21.9% confirmed credibly that they had been victims of cyberstalking for a longer time. (McFarlane & Bocij, 2003)

The consequences for the victims are disastrous. Victims suffer from trauma symptoms such as tension, sadness, anxiety, panic, insomnia, distrust and fear of men/women, and even post-traumatic stress disorder. (Sheridan, 2010) The literature knows of psychological damage from stalking behaviour, whether performed offline or online. It should not be forgotten, however, that the victims could also be expected to suffer financial damage. On the one hand, affected accounts have to be restored; sometimes the victim has to obtain a completely new digital identity and not to forget the costs that could result from a possible court hearing.

Nevertheless, many victims underestimate the consequences and do not report the crime. There can be different reasons for this. When cyberstalking occurs out of a past or current relationship, victims have an inhibition to report the crime to an authority. According to Huber (Huber, 2012), a maximum of 10% of cyberstalking victims are willing to report the crime. This low willingness of reporting the crime has its roots in being afraid of further acts of revenge or the victims are concerned that the cyberstalking activity can develop into a form of physical violence. Another motive for not reporting the cases is that many victims have difficulties to prove persistent persecution and threats that affect their lives in a negative way. (Huber, 2012) For example, the offender can share a video about a victim just once on YouTube. This action has a wide impact and may lead to a situation where a victim feels permanently threatened. The problem is that from this single case, the victim will find it difficult to prove persistent persecution or threat that has a degenerating affect his or her life. This problem can be solved only by improving the laws that have already been implemented in some countries.

SOLUTIONS AND RECOMMENDATIONS: WHAT IS THE TYPICAL COURSE OF ACTION (MODUS OPERANDI)?

Based on the hypothesis that the cyberstalking motif determines the course of action, this chapter will describe the methods, techniques, and typical behaviour in the course of action. With increasing digitalization, the modes operandi have also changed. This is not a special feature when dealing with stalking and cyberstalking in concrete terms. The development of crime in the last 30 years shows an increasing digitalization and change of the modus operandi in many areas. From an investigative point of view, it is interesting which methods the offenders choose to carry out their crime. This helps the investigating authorities to more easily identify the criminals and uncover cyberstalking.

Modus Operandi From Classical Stalking to Cyberstalking Research

As already discussed in the previous chapters, classical stalking very often takes place in a family, domestic or familiar environment. (Hoffmann, 2006) (Pathe & Mullen, 1997) As a result, perpetrators usually know the everyday life of the victim well and therefore choose the method that threatens or harasses the victim the most. In a representative study, it was found that the stalking method is strongly related to the stalking motif. (Huber, 2012) In all analyzed cases, there were no significant correlations to mental illnesses.

Cyberstalking of Private Individuals from the Motif of Unfulfilled Love

A typical pattern is that the suspect makes personal contact with the victim in a first step. This occurs in more than two thirds of all cases. (Huber, 2012) This occurs in the typically known communication channel, as perpetrator and victim usually communicate with each other. Whereas about 10 years ago it was SMS, telephone calls or e-mail, now it is messenger services such as Facebook Messenger, WhatsApp, Viber or Skype. If the communication does not have the desired effect, methods that are more aggressive are used. Especially in connection with domestic violence, technical tools such as espionage apps are used. The perpetrators install these apps on the victim's smartphone. In this way, they can constantly monitor where the victim is. Developments in recent years have shown that more and more perpetrators are gaining access to IoT devices.

This can be illustrated by an example from an Austrian court case: "A married couple divides. The ex-husband cannot cope with the divorce and wants to take revenge on the ex-wife. Although he has already moved out of the shared household, he still has access to the house's Internet-based control systems. In revenge he turns the victim's heating on in the summer and the light on and off in the night. Since he also managed the systems in the marriage together, he changed the access data to this control system immediately after moving out. The wife had no choice but to file a court order for omission." (Huber & Pospisil, 2017) In this example, the perpetrator and the victim are known to each other. In many escalation scenarios of such cases, intimate photos of the ex-partner are shared on social media platforms such as Facebook and Instagram. In contrast to situations where offender and victim are / were acquainted also, a few cases of cyberstalking are known in which the offender and victim do not know each other personally. This occurs, for example, with people who are in the public eye, such as actors or politicians. In these situations, it is often the case that the perpetrator illegally obtains access data to private accounts or mobile phones and harasses the victim with messages.

Revenge - Crime: Cyberstalking Because of Revenge Motives

Cyberstalking does not always result from an unfulfilled love. In addition, personal feelings of revenge out of professional or other private contexts can end in cyberstalking. The above mentioned court file analysis of all cybercrimes cases in Austria from 2006 to 2016 has shown that 43% of all cases (reported as well as unreported) fall within the area of revenge crime. (Huber, Pospisil & Seböck, 2018)

Commercial Cyberstalkers - Romance-Scams

Romance scams are a more recent development. They are regarded as a specific version of cyberstalking. The typical course of events is as follows:

In a first step, victims are addressed by perpetrators via social media platforms. Over a longer period, the perpetrator tries to establish a virtual but personal relationship with the victim. The goal of the criminal is to get so familiar with the victim that she or he sends private photos or videos to the delinquent. If these materials contain compromising content, the criminal has what he wants. Usually, the social media profile is deleted shortly afterwards. A few days later, the victim is blackmailed. If the victim does not pay, the pictures or videos are made available to the family, the employer or the public. (Europol, 2018) These perpetrators correspond to the profile of the classic cybercriminal. They often act from abroad. They can camouflage themselves very well and always operate out of a criminal group.

FUTURE RESEARCH DIRECTIONS

In summary, it can be said that cyberstalking is still a fuzzy term. The accurate meaning of cyberstalking is dependent of the legal, cultural, technical, social or psychological perspective from which the subject is investigated. Therefore, we can identify conceptual overlaps with cyberbullying, hate postings or other communicative violence on the Internet.

In general, it can be said that the use of modern telecommunication technologies makes it for offenders easier to stay anonymous. Encryption techniques such as Tor or VPN make it easier for perpetrators to be anonymous. The perpetrators can be found in all areas of life. Besides the expansion of classical stalking into the cyber area, revenge-crime can also be found in the professional environment. In addition, cybercriminal methods, such as romance scams, have developed which use cyberstalking as a business model.

As can be seen from the above, cyberstalking can be regarded as an offence with different causes and manifestations. On the one hand, digitalisation has brought about a change in media usage behaviour, while the constant availability of networked end devices makes it easier to become a perpetrator or victim of cyberstalking. With the increasing digitalisation and spread of IoTs, more opportunities for threatening victims have been created. As previous trends in cyberstalking have shown, there are different strategies perpetrators can use to approach their victims, which also poses new challenges to cyber security. Cyberstalking perpetrators use software and hardware devices to monitor their victims (e.g. Spyware). A proper password and device protection is therefore as indispensable as comprehensive prevention work.

CONCLUSION

3

Therefore, countermeasures are very important. In order to take preventive action against cyberstalking, several dimensions have to be considered. On the one hand, cybersecurity measures have to be put in place so that one's own computer system and its access data are protected. This is especially true for private individuals, who often gullibly provide their access data to various online systems to partners or acquaintances. On the other hand, society has to deal with these social developments and the communicative violence behind it. Education in schools and the promotion of netiquette is therefore indispensable. In addition, we have to start a political discussion regarding the rapid development of technology. It should be common knowledge that private individuals should avoid posting private information publicly on social media platforms such as Facebook, WhatsApp or Instagram. Above all, sensitive data such as telephone numbers, addresses and other personal information must not be published. In addition, effective password protection for private online accounts is necessary. Passwords should also be changed at regular intervals, especially if you have separated after a partnership. To make sure that there are no pictures or videos of yourself in circulation, you should google yourself regularly. To protect yourself from professional cyberstalking, good security software is needed, in order to protect your mobile devices from spyware or hacker attacks. One of the most important things is not to show too much credulity towards unknown people you meet on the internet. Furthermore, it is important to see recognize cyberstalking as a type of cybercrime. This requires taking the cultural aspects of each country and the current standards of cyber security into account.

REFERENCES

- nA.: Oberösterreichische Nachrichten. (2018, December 5). *Cyber-Stalker ließ 55-jährige Frau im Internet sterben und meldete sie ab. Oberösterreichische Nachrichten*. Retrieved from <https://www.nachrichten.at/oberoesterreich/steyr/Cyber-Stalker-liess-55-jaehrige-Frau-im-Internet-sterben-und-meldete-sie-ab;art68,3071034>
- Bocij, P. (2006). *The dark side of Internet: Protecting Yourself and your Family from Online Criminals*. Westport, CT: Praeger Pubischer.
- Döllinger, D. (1984). Probleme der Aktenanalyse in der Kriminologie. In *Methodologische Probleme in der kriminologischen Forschungspraxis* (pp. 265–286). Heidelberg, Germany: Academic Press.
- Dressing, H., & Foerster, K. (2010). Erotomanie, pathologische Verliebtheit, kognitive Distorsionen: Psychopathologische Übergänge beim Stalking. *Forensische Psychiatrie, Psychologie, Kriminologie*, 4(3), 155–159. doi:10.1007/11757-010-0058-3
- Dressing, H., Kühner, C., & Gass, P. (2005). Lifetime prevalence and impact of stalking in a European population: Epidemiological data from a middle-sized German City. *The British Journal of Psychiatry*, 187(AUG), 168–172. doi:10.1192/bjp.187.2.168 PMID:16055829
- Dressing, H., Kühner, C., & Gass, P. (2007). Multiaxiale Klassifikation von Stalkingfällen. *Der Nervenarzt*, 78(7), 764–772. doi:10.1007/00115-006-2205-9 PMID:17119890
- DugganM. (2017). *Online Harassment 2017*. Retrieved from http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf

- Europol, E. P. O. (2018). *Take Control of Your Digital Life. Don't be a Victim of Cyberscams!* Retrieved December 4, 2018, from <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don't-be-victim-of-cyber-scams>
- Forgo, N. (2010). Juristische Untersuchung. In *Forschungsbericht – Cyberstalking – Österreichweite Studie zum Cyberstalking-Verhalten* (p. 155). Wien: Huber.
- Goodno, N. H. (2007). Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws. *Missouri Law Review*, 72(1), 1–74.
- Hoffmann, J. (2006). *Stalking*. Heidelberg, Germany: Springer.
- Huber, E. (2012). *Cyberstalking und Cybercrime - kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher*. Wiesbaden: Springer.
- Huber, E. (2019). *Cybercrime - Eine Einführung*. Wiesbaden: Springer. doi:10.1007/978-3-658-26150-4
- Huber, E., & Pospisil, B. (2017). Die Cyber-Kriminellen in Wien. Eine Analyse von 2006-2016. Krems an der Donau: tredition GmbH.
- Huber, E., Pospisil, B., & Seböck, W. (2018). Without a trace - Cybercrime how are the offenders. In *DeepSec*. Retrieved from https://www.researchgate.net/publication/329321526_Without_a_Trace-Cybercrime_Who_are_the_Offenders
- INTEGRAL. (2010). AIM -Austrian Internet Monitor, rep. Österr. ab 14 Jahren, April bis Juni 2010, n= 3 000 pro Quartal. Wien: Author.
- INTEGRAL. (2018). AIM 2. *Quartal/2018*. Retrieved from https://www.integral.co.at/downloads/Internet/2018/07/AIM-C_-_Q2_2018.pdf
- Klicksafe.de. (2018). *Cyber-Mobbing – was ist das?* McClelland. (1987). *Human Motivation*. Cambridge University Press.
- McFarlane, L., & Bocij, P. (2003). Towards a typology of cyberstalkers. *First Monday*, 8(9). doi:10.5210/fm.v8i9.1076
- Mullen, P. E., & Pathe, M. P. R. (2000). *Stalkers and their victims*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9781139106863
- Nissenbaum, H. (2004). *Privacy as contextual integrity*. *Wash. L. Rev.* doi:10.1109/SP.2006.32
- Pathe, M., & Mullen, P. E. (1997). The impact of stalkers on their victims. *The British Journal of Psychiatry*, 170(JAN), 12–17. doi:10.1192/bjp.170.1.12 PMID:9068768
- Paul, B., & Leroy, M. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, (139), 31.
- Schneider, C., & Leest, U. (2018). *Gefahr, Mobbing und Cybermobbing bei Erwachsenen – die allgegenwärtige Gefahr*. Academic Press.
- Sheridan, L. L. A., & Lyndon, A. E. (2010). The influence of prior relationship, gender, and fear on the consequences of stalking victimization. *Sex Roles*, 66(5-6), 340–350. doi:10.1007/11199-010-9889-9

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, 4(1), 71–92. doi:10.1177/14614440222226271

Storey, J. E., & Hart, S. D. (2011). How Do Police Respond to Stalking? An Examination of the Risk Management Strategies and Tactics Used in a Specialized Anti-Stalking Law Enforcement Unit. *Journal of Police and Criminal Psychology*, 26(2), 128–142. doi:10.1007/11896-010-9081-8

Tokunaga, R. S., & Aune, K. S. (2017). Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking. *Journal of Interpersonal Violence*, 32(10), 1451–1475. doi:10.1177/0886260515589564 PMID:26082443

US Attorney General. (1999). *Cyberstalking: A new challenge for law enforcement and industry*. Author.

ADDITIONAL READING

Chawki, M., Darwish, A., Khan, A. A., & Sapna Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer. doi:10.1007/978-3-319-15150-2

Clifford, R. D. (2011). *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime*. Carolina Academic Press.

Curtis, G. (2011). *The Law of Cybercrimes and Their Investigations* (1st ed.). CRC Press. doi:10.1201/b13651

Hill, J. B., & Marion, N. E. (2016). *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. Praeger.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction*. Routledge. doi:10.4324/9781315296975

Koops, B.-J., & Brenner, S. (2006). *Cybercrime and Jurisdiction. A Global Survey*. Springer. doi:10.1007/978-90-6704-467-7

KEY TERMS AND DEFINITIONS

Brightfield: All criminal cases in a particular area known to the authorities.

Commerical Cyberstalker: A perpetrator who engage in cyberstalking for the purpose of financial gain.

Cyberstalking: A obsessive persecution or harassment of another person using IKT.

Darkfield: All criminal cases, in a certain area, that are not known to the authorities.

Modus Operandi: The typical course of events in a criminal offence.

Private Cyberstalker: A perpetrator of cyberstalking for personal motives.

Romance Scams: Social media are used to establish a relationship of trust between the perpetrator and the victim. As soon as the victim transmits confidential pictures or videos to the perpetrator, the perpetrator abuses them for blackmail purposes.

The Nature of Cyberbullying Among Youths

Michelle F. Wright

Penn State University, USA

INTRODUCTION

Millions of youths use electronic technologies, such as mobile phones and the Internet, daily (Lenhart, 2015). These technologies allow youths many opportunities, such as the ability to communicate with just about anyone, quick access to information for leisure and homework purposes, and entertainment (e.g., watching videos). Despite the positives associated with electronic technology use, many youths are at risk for exposure to problematic online situations. Such situations might involve viewing unwanted electronic content through videos, images, and text, which contains gory or sexually graphic content. Problematic online situations also include experiencing identity theft and being targeted by sexual predators. Cyberbullying is another risk associated with youths' electronic technology use.

Defined as an extension of traditional bullying, cyberbullying involves being targeted by negative and unwanted behaviors via electronic technologies, including email, instant messaging, social networking websites, and text messages via mobile phones (Bauman, Underwood, & Card, 2013; Grigg, 2012). The anonymity of the cyber context allows cyberbullies greater flexibility to harm their victims without having to witness the reactions of the victims and/or experience any negative consequences as a result of their actions (Wright, 2014b). Cyberbullies' ability to remain anonymous is made possible by the ability to mask or hide their identity in cyberspace. Because youths can remain anonymous online, anonymity can trigger the online disinhibition effect. The online disinhibition effect is when youths do or say something to others that they typically would never do or say in the offline world (Suler, 2004; Wright, 2014). Another component of electronic technologies is the rapid transmission of communication. Because electronic technologies have such a feature, many cyberbullies can target their victims more quickly. For example, a rumor in the offline world might take several hours to spread around school, while in the online world, this rumor could take a matter of minutes to spread to various classmates. Bullies can often target victims as often as they want as it is difficult to escape bullying in the online world as the behaviors can follow the person almost anywhere there is electronic technology access. Although it is possible to have many bystanders for traditional school bullying, cyberbullying has the potential to reach an audience of millions. These individuals can then perpetuate the cycle of cyberbullying by further sharing cyberbullying content (e.g., videos, pictures) with others.

The aim of this chapter is to review the topic of cyberbullying among youths, who might include children and adolescents from elementary school to high school. The literature reviewed includes studies from various disciplines, such as psychology, education, media studies, communication, social work, sociology, computer science, information technology, and gender studies. These studies might also include cross-sectional, longitudinal, qualitative, quantitative, and mixed-methods research designs. The chapter also draws on various studies across the world to conceptualize cyberbullying as a global health concern. The chapter includes seven sections, including:

DOI: 10.4018/978-1-5225-9715-5.ch044

1. **Background:** Contains the definition of cyberbullying, the various characteristic behaviors, the various electronic technologies, the prevalence rates of cyberbullying, and the role of anonymity in perpetrating cyberbullying.
2. **Youths' Characteristics and Risk Factors:** Reviews the factors associated with youths' involvement in cyberbullying as perpetrators and/or victims.
3. **Negative Psychosocial and Academic Outcomes:** Explains research findings regarding the psychological, social, behavioral, and academic consequences associated with youths' cyberbullying involvement.
4. **Theoretical Framework:** Provides an overview of the social cognitive theory and the online disinhibition effect, and their application to cyberbullying.
5. **Solutions and Recommendations:** This section describes suggestions for prevention and intervention programs aimed at reducing cyberbullying involvement among youths, and public policy recommendations.
6. **Future Research Directions:** Explains various recommendations for future research aimed at understanding youths' involvement in cyberbullying.
7. **Conclusion:** Highlights closing remarks regarding the current nature of the literature on cyberbullying.

BACKGROUND

Smith and colleagues (2013) defined cyberbullying as youths' use of electronic technologies to harass, embarrass, and intimidate others with hostile intent. The "hostile intent" portion of the definition is a requirement for a particular behavior or behaviors to qualify as cyberbullying. Cyberbullying can also include repetition and an imbalance of power between the perpetrator and the victim, similar to the traditional face-to-face bullying definition. In cyberbullying, the bully might target the victim multiple times by sharing a humiliating and embarrassing video or text message to one person or multiple people (Bauman et al., 2013). It might also include only sending a message to someone once. Another opportunity for repetitiveness might be sending a video or a text message to one person and then that particular person shares the content again with another person or multiple people, who then again share the content with someone else. Repetitiveness of cyberbullying captures the potentially cyclic nature of this form of bullying.

The electronic technology component of the cyberbullying definition separates this form of bullying from traditional face-to-face bullying (Curelaru, Iacob, & Abalasi, 2009). Examples of cyberbullying include sending unkind, mean, and/or nasty text messages, chat program messages, and emails, theft of identity information, pretending to be someone else, making anonymous phone calls, sharing secrets about the victim by posting or sending the secret to someone else, tricking someone to share a secret and then spreading the secret around, spreading nasty and/or untrue rumors using social networking websites, threatening to harm someone in the offline world, or uploading an embarrassing picture or video of a video who does not want the image shared (Bauman et al., 2013). Many cyberbullying behaviors are similar to those perpetrated or experienced in the offline world, such as experiencing/perpetrating harassment, insults, verbal attacks, teasing, physical threats, social exclusion, gossip, and humiliation.

Cyberbullying behaviors can occur through a variety of technologies, such as social networking websites, text messages via mobile phones, chat programs, online gaming, creation of a defamatory website against someone, and making fake social networking profiles using someone else's identity (Rideout et al., 2005). Another type of cyberbullying includes happy slapping, which involves a group of people

who insult another person at random while filming the incident via a mobile phone and then posting the images or videos online for others to watch. Flaming is another type of cyberbullying behavior, and it involves posting a provocative or offensive message in a public forum with the desire of provoking a hostile response or triggering an argument with other members of the forum. The most frequently utilized technologies to harm others include gaming consoles, instant messaging tools, and social networking websites (Ybarra et al., 2007).

The prevalence rates of cyberbullying among youths has been frequently examined. In one study, 3,767 middle school students (aged 11-14) were surveyed to examine their involvement in cyberbullying (Kowalski & Limber, 2007). Of this sample, 11% reported that they were cyberbullied at least once, 4% had bullied other youths, and 7% were involved as both perpetrator and victim. Higher prevalence rates were found by Patchin and Hinduja (2006). They found that 29% of the youths in their sample reported having experienced cyber victimization and 47% indicated that they were cyberbystanders. With an older sample of youths, grades 9th through 12th, Goebert and colleagues (2011) found that 56.1% of youths in their sample from the state of Hawaii reported that they were victims of cyberbullying. Taking into account the potential of cyberbullying experiences to extend from middle school to high school, Hinduja and Patchin (2012) surveyed youths in grades 6th through 12th. They found that 4.9% of their sample perpetrated cyberbullying in the past 30 days. Although differences in prevalence rates are the result of variations in sampling techniques and measurement techniques, it is important to understand these rates as they suggest that cyberbullying is a growing concern among children and adolescents. Cyberbullying is not just a problem localized to youths in the United States. Instead, it is a global problem with increasing evidence that cyberbullying occurs in Canada, Europe, Australia, Africa, Asia, and South America.

Cyberbullying in Canada

In comparison to cyberbullying prevalence rates in the United States, rates of youths' involvement in these behaviors is lower in Canada. In particular, Cappadocia and colleagues (2013) found that 2.1% of youths in their sample of 10th graders reported that they were perpetrators of cyberbullying, 1.9% reported being cybervictims, and 0.6% explained that they were both cyberbullies and cybervictims. Slightly higher rates were found in another sample of Canadian adolescents in the 8th through 10th grades (Bonnanno & Hymel, 2013). Bonnanno and Hymel found that 6% of their sample reported that they were cyberbullies, 5.8% reported that they were cybervictims only, and 5% indicated that they were both cyberbullies and cybervictims.

Cyberbullying in Europe

Using a sample of 22,544 Swedish youths, between the ages of 15 and 18, Laftman and colleagues (2013) found that 5% of their sample were cybervictims, 4% were cyberbullies, and 2% were both cybervictims and cyberbullies. In a slightly younger sample of Swedish adolescents, 7th through 9th graders, Beckman and colleagues (2012) found that 1.9% of their sample were cybervictims, 2.9% were classified as cyberbullies, and 0.6% were cyberbullies and cybervictims. Cyberbullying has also been documented in Ireland in a sample of 876 12 through 17 year olds (Corcoran, Connolly, & O'Moore, 2012). Rates were 6% for cyber victimization among this group of Irish youths. Italian youths typically report higher levels of cyberbullying involvement when compared to youths in Northern and Western Europe. In one study, Brighi et al. (2012) found that 12.5% of the Italian youths in their sample of 2,326, with an average age of 13.9 years, were classified as cybervictims. Similar rates have been found among German

youths. In this research, Festl and colleagues (2013) found that 13% of their sample of 276 13 through 19 year olds were classified as cyberbullies and 11% were classified as cybervictims. Olenik-Shemesh et al. (2010) found that 16.5% of their participants ($N = 242$; 13-16 year olds) were cybervictims. The rate of Israeli adolescents identified as cybervictims or witnesses of cyberbullying was 32.4% of the sample ($N = 355$; 13 to 17 year olds; Lazuras et al., 2013).

Research has also been conducted with Turkish youths. In this research, Yimaz (2011) found that 18% of the 756 7th graders in the study reported that they were victimized by cyberbullying and 6% reported that they were perpetrators of cyberbullying. Rates were much higher in Erdur-Baker's (2010) study. She found that 32% of the 276 youths, ages 14 to 18 years, in her study reported that they were cybervictims. Ayas and Horzum (2012) found that 19% of youths in the sample of 12 to 14 year olds had perpetrated cyberbullying. Slightly higher rates of cyberbullying perpetration were reported among Aricak et al.'s (2008) sample of 269 Turkish secondary school students. Of these students, 36% admitted that they had cyberbullied someone at least once.

Cyberbullying in Asia

Research on cyberbullying among Asian countries has been slower to develop than research in the United States, Canada, and Europe. In this research, Huang and Chou (2010) found that 63.4% of the 545 Taiwanese youths in their sample had witnessed cyberbullying, 34.9% were classified as cybervictims, and 20.4% were classified as cyberbullies. Jang and colleagues (2014) surveyed 3,238 Korean adolescents, with findings revealing that 43% were classified as being involved in cyberbullying. Similar rates have been found among adolescents in China, with 34.8% in one sample ($N = 1,438$) reporting that they were cyberbullies and 56.9% as cybervictims (Zhou et al., 2013). Focusing exclusively on Facebook cyberbullying, Kwan and Skoric (2013) reported that 59.4% of Singaporean adolescents in their study experienced cyber victimization through this social media website, while 56.9% perpetrated cyberbullying. In addition, Wong and colleagues (2014) found that 12.2% of adolescents in their sample ($N = 1,912$) were cybervictims and 13.1% were classified as cyberbullying perpetrators.

Cross-Cultural Differences in Cyberbullying Involvement

Research on the cross-cultural differences in cyberbullying typically classified countries according to an independent self-construal or an interdependent self-construal. To have an independent self-construal view, the self is viewed as separate from the social context. On the other hand, someone with an interdependent self-construal views themselves within the context of their society. Typically people from Western countries, like the United States, Canada, and the United Kingdom, reinforce and prime people to behave in ways aligned with an independent self-construal, while people from Eastern countries, like China, Korea, and Japan, are reinforced and primed for behavior consistently in regards to an independent self-construal. Differences in these self-construals affect people's social behaviors, particularly bullying and cyberbullying. Therefore, independent and interdependent self-construals have been used to explain these behaviors. In this research, youths from the United States typically reported higher rates of cyberbullying involvement, either as perpetrators or victims, when compared to Japanese youths (Barlett et al., 2013). Similar patterns have also been found among Austrian and Japanese youths (Strohmeier, Aoyama, Gradinger, & Toda, 2013). In other research, Chinese youths reported less cyberbullying perpetration when compared to Canadian youths (Li, 2008) but more cyberbullying victimization than Canadian youths (Li, 2006). Other research comparing East Asian youths from Canada with Canadian youths, Shapka

and Law (2013) found that East Asian youths engaged in cyberbullying more for proactive reasons (i.e., to obtain a goal), while Canadian youths reported cyberbullying perpetration for reactive reasons (i.e., response to provocation). Wright and colleagues (2015) found that Indian youths reported higher levels of cyberbullying involvement than youths from China and Japan, with Indian boys reporting the highest rates of cyberbullying involvement. Conducted in European countries, Genta and colleagues (2012) compared rates of cyberbullying perpetration among youths in Italy, Spain, and England. The findings revealed that Italian boys perpetrated more cyberbullying than boys from Spain and England.

YOUTHS' CHARACTERISTICS AND RISK FACTORS FOR CYBERBULLYING

Despite differences in the estimates of cyberbullying rates, these studies provided evidence that cyberbullying is an experience that is reported among youths. With the recognition that cyberbullying is something to be concerned about among youths, researchers began to direct their attention to the characteristics and risk factors related to youths' involvement in cyberbullying.

Age was one of the first risk factors to receive attention. Findings from this research indicated that cyberbullying victimization peaked in early adolescences and that high school adolescents were more likely to perpetrated cyberbullying (Williams & Guerra, 2007). In addition, physical forms of cyberbullying, such as hacking, also peaked in middle school but generally declined in high school. On the other hand, Wade and Beran (2011) concluded that cyberbullying involvement was highest among 9th graders in their study when compared to middle school students.

Other research has focused on gender as a predictor of youths' cyberbullying involvement. Findings from this research indicated that boys were more often the perpetrators of cyberbullying when compared to girls (Boulton et al., 2012; Li, 2007; Ybarra et al., 2007). In contrast, other research (e.g., Dehue, Bolman, & Vollink, 2008; Pornari & Wood, 2010) has revealed that girls were more often cyberbullies than boys. In some studies, girls reported that they were more often victimized by cyberbullying in comparison to boys (Hinduja & Patchin, 2007; Kowalski & Limber, 2007). Contrary to these findings, some research (e.g., Huang & Chou, 2010; Sjurso, Fandrem, & Roland, 2016) has found that boys were more often cybervictims when compared to girls. Other studies (e.g., Stoll & Block, 2015; Wright & Li, 2013b) have revealed no gender differences in youths' involvement in cyberbullying.

Researchers have also directed their attention to considering youths' offline experience of perpetrators and victims of traditional school bullying as risk factors for youths' involvement in cyberbullying. These studies have considered the role of victim and perpetrator in both the face-to-face and cyber contexts. In these studies, positive associations are found between cyberbullying perpetration and traditional face-to-face bullying perpetration, cyber victimization and traditional face-to-face victimization, and cyberbullying perpetration and traditional face-to-face victimization (Barlett & Gentile, 2012; Mitchell et al., 2007; Wright & Li, 2013a; Wright & Li, 2013b).

Another risk factor associated with youths' cyberbullying involvement is their use of electronic technology. The underlying conclusion in this research is that any exposure to electronic technology can increase youths' risk of cyberbullying. Higher use of the internet is associated positively with both the perpetration and victimization by cyber victimization (Ang, 2016; Aricak et al., 2008). Compared with nonvictims, cybervictims spend more time using instant messaging tools, email, blogging sites, and online gaming (Smith et al., 2008). A possible explanation for the connection between electronic technology use and cyberbullying involvement is the likelihood that these youths disclose more personal

information online, including geographical location (Ybarra et al., 2007). Disclosing this information puts them at risk for cyber victimization.

Internalizing problems, like depression and loneliness, as well as externalizing problems, like alcohol use, are also associated with youths' involvement in cyberbullying. To explain such relationships, researchers propose that victims' coping abilities are diminished or ineffective, which makes them vulnerable to cyberbullying (Cappadocia et al., 2013; Mitchell et al., 2007). Furthermore, Cappadocia and colleagues (2013) and Wright (in press) found that alcohol and drug use were each related positively to cyberbullying perpetration.

Researchers have also identified other variables that are linked to youths' cyberbullying involvement. Normative beliefs are the beliefs that a specific set of behavior, in this case cyberbullying, is an acceptable form of behavior. In this research, youths with higher normative beliefs concerning face-to-face bullying and cyberbullying were related positively to cyberbullying perpetration (e.g., Burton, Florell, & Wygant, 2013; Wright, 2014b). Therefore, cyberbullies believe that cyberbullying is an acceptable form of behavior to engage in. Provictim attitudes, defined as the belief that bullying is unacceptable and that defending victims is valuable, is another factor related to cyberbullying. Holding lower levels of provictim attitudes is associated positively with cyberbullying perpetration (Sevcikova, Machackova, Wright, Dedkova, & Cerna, 2015). In addition, youths with lower levels of peer attachment, less self-control, and empathy, and greater moral disengagement were each related positively to cyberbullying perpetration (e.g., Wright, Kamble, Lei, Li, Aoyama, & Shruti, 2015).

Many of the studies on the characteristics and risk factors associated with cyberbullying involvement utilize cross-sectional research designs. Consequently, it is difficult to make understand the long-term associations of these characteristics and risk factors associated with cyberbullying involvement. Fanti and colleagues (2012) conducted a longitudinal study investigating youths' exposure to violent media and their callous and unemotional traits in relation to cyberbullying involvement one year later. Findings revealed that media violence exposure related to greater cyber victimization. Perceived levels of stress from parents, peers, and academics also have a role in adolescents' perpetration of cyberbullying one year later (Wright, 2014a).

In sum, there are a variety of characteristics and risk factors that make youths vulnerable to cyberbullying. Moving away from individual-related characteristics and risk factors, other researchers have examined the role of parents, schools, and teachers in youths' cyberbullying involvement.

Parents as Risk Factors

Parenting styles are linked to youths' involvement in cyberbullying. In particular, youths who are bully-victims often have parents who utilize indifferent-uninvolved parenting styles and inconsistent monitoring of their activities increases youths' involvement in cyberbullying (Totura et al., 2009). Neglectful parenting, or sometimes referred to as indifferent-uninvolved parenting, increased youths' involvement in cyberbullying in comparison to uninvolved youths (Dehue, Bolman, Vollink, & Pouwelse, 2012). Indifferent-uninvolved parents are often emotionally distance from their children, engage in little or no supervision, show little warmth and affection toward their children, place fewer demands on their children's behaviors, might and intentionally avoid their children. Cyber victimization was also increased among children who reported that their parents engaged in authoritarian parenting styles. Authoritarian parenting style is defined as parents who have high levels of demands and low levels of responsiveness. These parents have very high expectation but they display very low levels of warmth or nurturance.

Another aspect of parenting is the use of parental monitoring. The cyber context provides another opportunity for parents to monitor their children's online activity. In this research, Mason (2008) found that 50% of the children in his study reported that their parents monitored their online activities. One study explored the differences between what parents report in terms of how often they monitor their children's online activities and how often their children reported being monitored (McQuade, Colt, & Meyer, 2009). McQuade et al. found that 93% of parents in their study reported that they set limits on their children's online activities. However, only 37% of their children reported that their parents had given them rules regarding their online activities. These findings might indicate that parents overestimate the amount of monitoring they engage in or that the strategies they do implement are ineffective. Just like in the offline world, parents have an important role in protecting their children against online risks. Additional attention should be given to how parents navigate conversations with their children about online risks and opportunities.

Other research has focused on the role of parental monitoring and parental mediation in relation to reducing youths' risk of cyberbullying involvement. Wright (2015) found that when youths reported more technology mediation by their parents they reported lower levels of cyber victimization and the associated negative adjustment difficulties. To explain these connections, Wright explains that parents who monitor their children's electronic technology use might have more opportunities to engage in discussions on the risks associated with cyberbullying involvement. Parents might also convey, during these discussions, that cyberbullying is unacceptable. Such a proposal is supported by the literature as Hinduja and Patchin (2013) and Wright (2013a) found that youths who were concerned with being punished for negative online behaviors were much less likely to perpetrate cyberbullying. One study found little support that parental monitoring was helpful for preventing cyberbullying involvement. In this study, Aoyama and colleagues (2011) did not find that parental mediation and monitoring of their children's online activities were related to their children's cyberbullying perpetration and victimization. Aoyama et al. explained that many parents lack the technological skills to effectively monitor their children's online activities, which makes it difficult for them to know when and how to intervene in these activities. Another potential explanation might be that parents implement rules for electronic technology use that they do not follow-up on. Not following through with these rules can give the impression that parents are unconcerned with appropriate online behaviors, increasing the risk of engaging in cyberbullying. Failing to enforce rules might also indicate that parents do not often update strategies as their children become more independent electronic technology users. Research findings support this proposal as many parents report that they are not sure as to what type of online activities to discuss with their children (Rosen, 2007). When parents are not sure how to talk to their children about online activities, then it might lead many parents to not discuss appropriate online behaviors with their children.

There is also some research which investigates other family characteristics in relation to youths' cyberbullying involvement. Family income, parental education, and marital status of caregivers were unrelated to youths' involvement in cyberbullying (Ybarra & Mitchell, 2004). Other research indicates that parental unemployment increased youths' risk of cyberbullying perpetration and victimization (Arslan, Savaser, Hallett, & Balci, 2012).

Schools as Risk Factors

Schools' role in monitoring and punishing youth's involvement in cyberbullying is a topic of great debate about school districts, parents, authorities, and researchers. This is because many of the cases involving cyberbullying are carried out off school groups, making it difficult for schools to be aware of such cases

(deLara, 2012; Mason, 2008). However, many incidences of cyberbullying involve youths who attend the same school, making the schools' role in handling such incidences complex. Because cyberbullies and cybervictims might attend the same school, it is possible that knowledge of a cyberbullying incidence could spread throughout the school, leading to negative interactions between youths while on school grounds. These negative interactions could disrupt the learning process.

Regardless of the extent to which cyberbullying incidences can “spill over” onto school grounds, many administrators, teachers, and school districts have very different perceptions and awareness of cyberbullying. Some of these individuals might not even perceive cyberbullying as a significant event, warranting attention (Kochenderfer-Ladd & Pelletier, 2008). It is problematic when administrators and teachers do not perceive cyberbullying as problematic because electronic technology and digital communication are embedded in the lives of the youths they teach. Furthermore, these administrators and teachers are often not likely to perceive any form of covert bullying behavior as serious and harmful as physical bullying (Sahin, 2010). They are often not likely to understand the consequences associated with relational bullying and cyberbullying. This could lead to the decision not to help youths who experience these behaviors or dealing with the situation by minimizing it. Teacher training might not properly inform teachers on how to deal with and recognize cyberbullying, making teachers' ability to intervene difficult. Cassidy et al. (2012a) found that many Canadian teachers were unfamiliar with newer technologies. Being unfamiliar with newer technologies made it difficult for these teachers to deal with cyberbullying as they were often unsure of how to respond to the incidence or of how to implement strategies to address the incident. Even when teachers were concerned with cyberbullying, their school district did not have policies and programs in place to deal with these behaviors (Cassidy, Brown, & Jackson, 2012b). This made it difficult for teachers to implement solutions and strategies.

Other research has revealed that teachers were often willing to participate in prevention programs aimed at reducing traditional face-to-face bullying but not cyberbullying prevention programs (Tangen & Campbell, 2010). This could be a product of few empirically and theoretical driven cyberbullying prevention programs or that administrators and teachers do not consider cyberbullying an important enough issue to warrant attention. Recognizing the importance of implementing policies and training programs on cyberbullying is important because youths' involvement in these behaviors has the potential to impact the learning environment (Shariff & Hoff, 2007).

Educators require training to increase their awareness of cyberbullying, with the hope of developing policies at the school level to reduce these behaviors. When teachers are more confident about their abilities and have a stronger commitment to their school, they are more likely to learn about cyberbullying, and have a greater awareness of these behaviors and knowledge to deal effectively with it (Eden et al., 2013). Such awareness and knowledge prevent children's and adolescents' cyberbullying perpetration and victimization. Furthermore, when teachers feel more confident, they intervene in cyberbullying incidences more often, which protects adolescents' from experiencing these behaviors (Elledge et al., 2013). Unfortunately, teachers' motivation for learning about cyberbullying decreases from elementary school to middle school, which is problematic as cyberbullying involvement usually increases in these years (Ybarra et al., 2007). Therefore, there is a need for educator training programs aimed at raising awareness of cyberbullying, particularly in the middle school years.

Youths' involvement in cyberbullying are less likely to perceive their school and teachers positively when compared to uninvolved youths (Bayar & Ucanok, 2012). Some youths might experience cyberbullying and fear that their classmates could be responsible. This decreases these youths' concentration on learning, thereby reducing their academic attainment and performance (Eden, Heiman, & Olenik-Shemesh, 2013). Lower school commitment and perceptions of a negative school climate increase children's and

adolescents' engagement in cyberbullying as they feel less connected to their school (Williams & Guerra, 2007). Youths' involvement in cyberbullying is linked to poor academic functioning (Wright, in press).

Peer interactions are present in both the offline and online world. Through these interactions, youths learn about the social norms dictating acceptable and unacceptable behaviors within the peer group, and consequently they engage in more of the acceptable behaviors, even if they are negative. In this line of research, cyberbullying involvement is highest among classrooms in which these behaviors are elevated (Festl et al., 2013). Something about the classroom climate might be driving the levels of cyberbullying behaviors within a particular classroom. Furthermore, believing that one's friends engaged in cyberbullying also increases youths' risk of perpetrating cyberbullying (Hinduja & Patchin, 2013). Peer contagion might potentially explain these relationships. What this means is that one's friends "spread" negative online behaviors to others within their social network (Sijtsema, Ashwin, Simona, & Gina, 2014).

Another peer-related variable associated with cyberbullying involvement is peer attachment. Peer attachment is defined as the closeness that youths feel with their same or similarly aged peers. Lower levels of peer attachment were associated positively with cyberbullying perpetration and victimization (Burton et al., 2013). When youths have poor peer attachment, they are likely to believe that their peers will not be there for them when they need it. This belief promotes negative interactions with peers. Cyberbullying involvement is higher when youths' experience peer rejection, whether perceived rejection or peer-reported rejection (Sevcikova et al., 2015; Wright & Li, 2013b). Wright and Li (2012) argue that peer rejection triggers negative emotional responses that leads to cyberbullying perpetration and victimization.

Cyberbullying perpetration might also be used to maintain and boost youths' social standing among their peer group, both online and offline. Wright (2014c) found that higher levels of perceived popularity, a reputational type of popularity in the peer group, was associated positively with cyberbullying perpetration six months later. With the prominent role of electronic technologies in youths' lives, Wright proposes that they might utilize these technologies as a tool for the promotion and maintenance of their social standing. The literature in this section suggests that it is important to consider the role of schools and peers in youths' cyberbullying involvement.

NEGATIVE PSYCHOSOCIAL AND ACADEMIC OUTCOMES THE OUTCOMES ASSOCIATED WITH YOUTHS' INVOLVEMENT IN CYBERBULLYING

Concerns with cyberbullying involvement among youths were triggered by the associated negative psychosocial and academic outcomes. A potential research for these linkages is that cyberbullying disrupts youths' emotional experiences, making them more vulnerable to negative outcomes, due to ineffective coping strategies. Cybervictims are more likely than nonvictims to report lower levels of global happiness, general school happiness, school satisfaction, family satisfaction, and self-satisfaction (Toledano, Werch, & Wiens, 2015). In addition, cybervictims report more feelings of anger, sadness, and fear in comparison to noninvolved children and adolescents (Dehue et al., 2008; Machackova, Dedkova, Sevcikova, & Cerna, 2013; Patchin & Hinduja, 2006).

Cyberbullying involvement also impacts youths' academic performance. In this literature, both cybervictims and cyberbullies are at an increased risk for difficulties at school, including academic problems, less motivation for school, poor academic performance, lower academic attainment, and more school absences (Belae & Hall, 2007; Yousef & Bellamy, 2015). Lower school functioning also relates to cyberbullying perpetration and cyber victimization (Wright, in press). Cyberbullies and cybervictims

experience the lower levels of school functioning when compared to cyberbullies, cybervictims, and uninvolved youths.

Internalizing and externalizing problems are both associated with youths' cyberbullying involvement (e.g., Mitchell, Ybarra, & Finkelhor, 2007; Patchin & Hinduja, 2006; Wright, 2014b; Ybarra, Diener-West, & Leaf, 2007). Cyberbullies and cybervictims both experience suicidal thoughts and attempt suicide more often than uninvolved youths (Bauman, Toomey, & Walker 2013). Similar results were found by Beckman and colleagues (2012). Beckman and colleagues also found that cyberbullying involvement increased youths' risk for experiencing mental health problems. Other research suggests that these youths are also at risk for psychiatric and psychosomatic problems (Sourander et al., 2010).

A limitation associated with the research on the psychosocial and behavioral consequences related to youths' cyberbullying involvement is that researchers do not account for youths' involvement in traditional face-to-face bullying. It is important to account for youths' involvement in traditional face-to-face bullying because this experience is associated with similar consequences as cyberbullying and due to the high correlation between the two (Williams & Guerra, 2007; Wright & Li, 2013b). One study accounted for traditional face-to-face bullying involvement and the findings suggested that cyberbullying perpetration and victimization might have worse psychological consequences when compared to the face-to-face bullying perpetration and victimization, after controlling for face-to-face bullying and victimization (Bonanno et al., 2013).

Given the high correlation between cyberbullying and traditional face-to-face bullying involvement, some researchers have focused on the combined effects of these experiences on youths' psychosocial and behavioral outcomes. In this research, victims of both traditional face-to-face bullying and cyberbullying reported higher levels of internalizing symptoms when compared to youths who experienced only one type of victimization (Gradinger et al., 2009; Perren et al., 2012).

The research reviewed in this section suggests that a combination of various bullying experiences, whether online or offline, exacerbates youths' experience of depression, anxiety, and loneliness. These findings indicate the importance of considering youths' involvement in various bullying behaviors to better understand the best ways to intervene.

THEORETICAL FRAMEWORKS

In this section, two theories will be presented, along with their application to cyberbullying involvement among youths. These theories include the social cognitive theory and the online disinhibition effect.

According to the social cognitive theory, parents and/or friends serve as important models of behaviors that are observed and replicated by youths (Hinduja & Patchin, 2008; Mouttapa, Valente, Gallaher, Rohrbach, & Unger, 2004). This theory has been extensively applied to youths' involvement in aggressive behaviors, including cyberbullying (Barlett & Gentile, 2012). According to Olweus (1993), children's aggressive behaviors are learned or modeled by someone who was stronger than the observer. The effects of the model on the observer depended on the observer's positive evaluation of the model. These perceptions have the potential to increase the likelihood of reducing children's inhibition for aggressive behaviors and increase aggressive acts, particularly when the model is rewarded for acting aggressively. In regard to cyberbullying, youths observe various incidences of successful cyberbullying acts (Barlett & Gentile, 2012). The more often they are exposed to these acts the greater the likelihood that they believe cyberbullying is acceptable, normative, and tolerable. The anonymity offered by the cyber context increases the chance that little or no immediate consequences occur after cyberbullying perpetration.

When youths are positively reinforced for cyberbullying behaviors, adolescents held greater positive attitudes toward these behaviors (Barlett & Gentile, 2012). These attitudes relate to future perpetration of cyberbullying behaviors (Wright & Li, 2013a; Wright & Li, 2013b).

The online disinhibition effect theory refers to the likelihood that the characteristics of the cyber context will increase the likelihood that youths engage in different ways online than they would offline (Suler, 2004). The cyber context allows people to loosen, reduce, or dismiss the typical social restrictions and inhibitions present in normal face-to-face interactions (Mason, 2008). The literature supports the premise that people behave differently in cyberspace than in the offline world. Research indicates that people are likely to be blunter when communicating with others via electronic technologies (McKenna & Bargh, 2000). In online communication, there are more misunderstanding, heightened hostility, and increase in aggressive behaviors via electronic technologies when compared to face-to-face communication. It is also possible for communications through some electronic technologies might to not see emotional reactions. Not being able to see someone's emotional reactions in cyberspace prevents people from modulating their own behaviors because they are not able to witness the consequences of their actions, like they could in the offline world (Kowalski & Limber, 2007). Cyberbullying often occurs because cyberbullies cannot witness the cybervictims' reactions nor are their many opportunities to experience social disapproval, punishment, or other consequences. Many cyberbullies recognize the ease of engaging in aggressive behaviors through electronic technologies, which could potentially lead their behaviors to become more disinhibited over time, especially when they receive positive reinforcement for their behavior and are not able to recognize the consequences of their behaviors (Hinduja & Patchin, 2010; Wright, 2014a). Deindividuation, the process of not being accountable for one's actions, also occurs as a result of the online disinhibition effect (Joinson, 1998). Being able to remain anonymous through electronic technologies reduces youths' accountability for their online interactions. Coupling the reduction of accountability with the anonymity of the cyber context, might make it easier for youths to disengage from others, leading to increases in harmful online behaviors (Wright, 2014a).

SOLUTIONS AND RECOMMENDATIONS

Cyberbullying is a public health concern, warranting attention by all members of our communities, including educators, researchers, parents, and youths themselves. It is also important for education curriculum to include digital literacy skills training and citizenship in both the online and offline worlds (Cassidy et al., 2012b). Such curriculum should also focus on the positive uses of electronic technology, building empathy for negative online interactions, self-esteem, and social skills. To also improve school climate, administrators and teachers should learn students' names, praise good behavior, and stay technologically informed and up-to-date (Hinduja & Patchin, 2012).

Schools and parents should partner to help address cyberbullying. Parents should also increase their awareness and knowledge of electronic technologies (Cassidy et al., 2012a; Diamanduros & Downs, 2011). Increasing one's knowledge of electronic technologies can help parents understand the importance of technology in their children's lives and to recognize the risk and opportunities of their children's electronic technology use. Parents can also implement more effective monitoring strategies when they are more knowledge about electronic technologies and cyberbullying. Parents are encouraged to engage in open dialogue with children about appropriate electronic technology use.

FUTURE RESEARCH DIRECTIONS

There are some noticeable future directions for research on youths' involvement in cyberbullying. Anonymity is associated with youths' perpetration of cyberbullying involvement, but little attention has been given to this topic. Future research should focus on youths' perceptions of anonymous acts online and which factors might motivate them to engage in anonymous forms of cyberbullying. This research should also examine anonymous forms of cyberbullying versus non-anonymous forms of cyberbullying to better understand the motivators underlying these behaviors. This research should also investigate whether coping strategies and psychosocial adjustment difficulties vary as a function of whether cyberbullying was anonymous or non-anonymous. Additional investigations should be undertaken to understand the long-term impact of cyberbullying involvement among youths. Intervention and prevention programs could be developed which specific consideration to the specific age group identified as at the most risk for cyberbullying involvement.

CONCLUSION

The literature in this chapter provides a firm foundation for understanding youths' involvement in cyberbullying and the next directions for intervention, prevention, public policy, and research. The review suggests that much of the earlier research on cyberbullying focused on the prevalence rates of these behaviors. Current shifts in this research has changed the focus to understanding the causes and consequences of youths' involvement in cyberbullying. Although this research is still in its early stages in comparison to the literature on traditional face-to-face bullying, many of the published studies on cyberbullying focus on individual predictors of youths' involvement in these behaviors. More consideration is needed to understand the role of parents, schools, peers, and communities in youths' cyberbullying perpetration and victimization. Follow-up research on cyberbullying is important as this negative behavior impacts many aspects of our society, potentially undermining ethical and moral values. Consequently, it is imperative that we unite and do our part to reduce children's and adolescents' involvement in cyberbullying together.

SUMMARY

The purpose of this literature review was to summarize research on cyberbullying involvement among youths by providing a description and definition, information about the characteristics and risk factors, the negative adjustment outcomes associated with the involvement in these behaviors, and theoretical frameworks. The studies reviewed in this chapter utilize cross-sectional, longitudinal, qualitative, quantitative, and mixed-methods research designs. Studies with various youths from across the world were also reviewed to shed more light on the cross-cultural research on youths' cyberbullying involvement. This cross-cultural research also provides support about youths' cyberbullying involvement being a global phenomenon.

REFERENCES

- Ang, R. P. (2016). Cyberbullying: Its prevention and intervention strategies. In D. Sibnath (Ed.), *Child safety, welfare and well-being: Issues and challenges* (pp. 25–38). New York: Springer. doi:10.1007/978-81-322-2425-9_3
- Aoyama, I., Utsumi, S., & Hasegawa, M. (2011). Cyberbullying in Japan: Cases, government reports, adolescent relational aggression and parental monitoring roles. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Bullying in the global playground: Research from an international perspective*. Oxford, UK: Wiley-Blackwell.
- Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *Cyberpsychology & Behavior*, 11(3), 253–261. doi:10.1089/cpb.2007.0016 PMID:18537493
- Arslan, S., Savaser, S., Hallett, V., & Balci, S. (2012). Cyberbullying among primary school students in Turkey: Self-reported prevalence and associations with home and school life. *Cyberpsychology, Behavior, and Social Networking*, 15(10), 527–533. doi:10.1089/cyber.2012.0207 PMID:23002988
- Ayas, T., & Horzum, M. B. (2010). *Cyberbullg / victim scale development study*. Retrieved from: <http://www.akademikbakis.org>
- Barlett, C. P., & Gentile, D. A. (2012). Long-term psychological predictors of cyber-bullying in late adolescence. *Psychology of Popular Media Culture*, 2, 123–135. doi:10.1037/a0028113
- Barlett, C. P., Gentile, D. A., Anderson, C. A., Suzuki, K., Sakamoto, A., Yamaoka, A., & Katsura, R. (2013). Cross-cultural differences in cyberbullying behavior: A short-term longitudinal study. *Journal of Cross-Cultural Psychology*, 45(2), 300–313. doi:10.1177/0022022113504622
- Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence*, 36(2), 341–350. doi:10.1016/j.adolescence.2012.12.001 PMID:23332116
- Bauman, S., Underwood, M. K., & Card, N. A. (2013). Definitions: Another perspective and a proposal for beginning with cyberaggression. In S. Bauman, D. Cross, & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, methodology* (pp. 26–40). New York, NY: Routledge.
- Bayar, Y., & Ucanok, Z. (2012). School social climate and generalized peer perception in traditional and cyberbullying status. *Educational Sciences: Theory and Practice*, 12, 2352–2358.
- Beckman, L., Hagquist, C., & Hellstrom, L. (2012). Does the association with psychosomatic health problems differ between cyberbullying and traditional bullying? *Emotional & Behavioural Difficulties*, 17(3-4), 421–434. doi:10.1080/13632752.2012.704228
- Bonanno, R. A., & Hymel, S. (2013). Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying. *Journal of Youth and Adolescence*, 42(5), 685–697. doi:10.1007/10964-013-9937-1 PMID:23512485
- Boulton, M., Lloyd, J., Down, J., & Marx, H. (2012). Predicting undergraduates' self-reported engagement in traditional and cyberbullying from attitudes. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 141–147. doi:10.1089/cyber.2011.0369 PMID:22304402

- Brighi, A., Guarini, A., Melotti, G., Galli, S., & Genta, M. L. (2012). Predictors of victimisation across direct bullying, indirect bullying and cyberbullying. *Emotional & Behavioural Difficulties*, 17(3-4), 375–388. doi:10.1080/13632752.2012.704684
- Burton, K. A., Florell, D., & Wygant, D. B. (2013). The role of peer attachment and normative beliefs about aggression on traditional bullying and cyberbullying. *Psychology in the Schools*, 50(2), 103–114. doi:10.1002/pits.21663
- Cappadocia, M. C., Craig, W. M., & Pepler, D. (2013). Cyberbullying: Prevalence, stability and risk factors during adolescence. *Canadian Journal of School Psychology*, 28(2), 171–192. doi:10.1177/0829573513491212
- Cassidy, W., Brown, K., & Jackson, M. (2012a). “Making kind cool”: Parents’ suggestions for preventing cyber bullying and fostering cyber kindness. *Journal of Educational Computing Research*, 46(4), 415–436. doi:10.2190/EC.46.4.f
- Cassidy, W., Brown, K., & Jackson, M. (2012b). “Under the radar”: Educators and cyberbullying in schools. *School Psychology International*, 33(5), 520–532. doi:10.1177/0143034312445245
- Corcoran, L., Connolly, I., & O’Moore, M. (2012). Cyberbullying in Irish schools: An investigation of personality and self-concept. *The Irish Journal of Psychology*, 33(4), 153–165. doi:10.1080/03033910.2012.677995
- Curelaru, M., Iacob, I., & Abalasei, B. (2009). *School bullying: Definition, characteristics, and intervention strategies*. Lumea Publishing House.
- Dehue, F., Bolman, C., & Vollink, T. (2008). Cyberbullying: Youngsters’ experiences and parental perception. *CyberPsychology & Behavior*, 11(2), 217–223. doi:10.1089/cpb.2007.0008 PMID:18422417
- Dehue, F., Bolman, C., Vollink, T., & Pouwelse, M. (2012). Cyberbullying and traditional bullying in relation to adolescents’ perceptions of parenting. *Journal of Cyber Therapy and Rehabilitation*, 5, 25–34.
- deLara, E. W. (2012). Why adolescents don’t disclose incidents of bullying and harassment. *Journal of School Violence*, 11(4), 288–305. doi:10.1080/15388220.2012.705931
- Diamanduros, T., & Downs, E. (2011). Creating a safe school environment: How to prevent cyberbullying at your school. *Library Media Connection*, 30(2), 36–38.
- Eden, S., Heiman, T., & Olenik-Shemesh, D. (2013). Teachers’ perceptions, beliefs and concerns about cyberbullying. *British Journal of Educational Technology*, 44(6), 1036–1052. doi:10.1111/j.1467-8535.2012.01363.x
- Elledge, L. C., Williford, A., Boulton, A. J., DePaolis, K. J., Little, T. D., & Salmivalli, C. (2013). Individual and contextual predictors of cyberbullying: The influence of children’s provictim attitudes and teachers’ ability to intervene. *Journal of Youth and Adolescence*, 42(5), 698–710. doi:10.1007/10964-013-9920-x PMID:23371005
- Erdur-Baker, O. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools. *New Media & Society*, 12(1), 109–125. doi:10.1177/1461444809341260

- Fanti, K. A., Demetriou, A. G., & Hawa, V. V. (2012). A longitudinal study of cyberbullying: Examining risk and protective factors. *European Journal of Developmental Psychology*, 8(2), 168–181. doi:10.1080/17405629.2011.643169
- Festl, R., Schwarkow, M., & Quandt, T. (2013). Peer influence, internet use and cyberbullying: A comparison of different context effects among German adolescents. *Journal of Children and Media*, 7(4), 446–462. doi:10.1080/17482798.2013.781514
- Goebert, D., Else, I., Matsu, C., Chung-Do, J., & Chang, J. Y. (2011). The impact of cyberbullying on substance use and mental health in a multiethnic sample. *Maternal and Child Health Journal*, 15(8), 1282–1286. doi:10.1007/10995-010-0672-x PMID:20824318
- Grading, P., Strohmeier, D., & Spiel, C. (2009). Traditional bullying and cyberbullying. *The Journal of Psychology*, 217, 205–213.
- Grigg, D. W. (2012). Definitional constructs of cyberbullying and cyber aggression from a triagnulatory overview: A preliminary study into elements. *Journal of Aggression, Conflict and Peace Research*, 4(4), 202–215. doi:10.1108/17596591211270699
- Hinduja, S., & Patchin, J. W. (2007). Offline consequences of online victimization. *Journal of School Violence*, 6(3), 89–112. doi:10.1300/J202v06n03_06
- Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29(2), 129–156. doi:10.1080/01639620701457816
- Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206–221. doi:10.1080/13811118.2010.494133 PMID:20658375
- Hinduja, S., & Patchin, J. W. (2012). Cyberbullying: Neither and epidemic nor a rarity. *European Journal of Developmental Psychology*, 9(5), 539–543. doi:10.1080/17405629.2012.706448
- Hinduja, S., & Patchin, J. W. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of Youth and Adolescence*, 42(5), 711–722. doi:10.1007/10964-012-9902-4 PMID:23296318
- Huang, Y., & Chou, C. (2010). An analysis of multiple factors of cyberbullying among junior high school students in Taiwan. *Computers in Human Behavior*, 26(6), 1581–1590. doi:10.1016/j.chb.2010.06.005
- Jang, H., Song, J., & Kim, R. (2014). Does the offline bully-victimization influence cyberbullying behavior among youths? Application of general strain theory. *Computers in Human Behavior*, 31, 85–93. doi:10.1016/j.chb.2013.10.007
- Joinson, A. (1998). Causes and implications of behavior on the Internet. In J. Gackenbach (Ed.), *Psychology and the Internet: Intrapersonal, interpersonal, and transpersonal implications* (pp. 43–60). San Diego, CA: Academic Press.
- Kochenderfer-Ladd, B., & Pelletier, M. (2008). Teachers' views and beliefs about bullying: Influences on classroom management strategies and students' coping with peer victimization. *Journal of School Psychology*, 46(4), 431–453. doi:10.1016/j.jsp.2007.07.005 PMID:19083367
- Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *The Journal of Adolescent Health*, 41(6), 22–30. doi:10.1016/j.jadohealth.2007.08.017 PMID:18047942

- Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in Human Behavior*, 29(1), 16–25. doi:10.1016/j.chb.2012.07.014
- Laftman, S. B., Modin, B., & Ostberg, V. (2013). Cyberbullying and subjective health: A large-scale study of students in Stockholm, Sweden. *Children and Youth Services Review*, 35(1), 112–119. doi:10.1016/j.chldyouth.2012.10.020
- Lazuras, L., Barkoukis, V., Ourda, D., & Tsorbatzoudis, H. (2013). A process model of cyberbullying in adolescence. *Computers in Human Behavior*, 29(3), 881–887. doi:10.1016/j.chb.2012.12.015
- Lenhart, A. (2015). *Teens, social media & technology overview 2015*. Retrieved from: <http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/>
- Li, Q. (2007). Bullying in the new playground: Research into cyberbullying and cybervictimization. *Australian Journal of Educational Technology*, 23, 435–454.
- Li, Q. (2008). A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Research*, 50(3), 223–234. doi:10.1080/00131880802309333
- Machackova, H., Dedkova, L., & Mezulanikova, K. (2015). Brief report: The bystander effect in cyberbullying incidents. *Journal of Adolescence*, 43, 96–99. doi:10.1016/j.adolescence.2015.05.010 PMID:26070168
- Machackova, H., Dedkova, L., Sevcikova, A., & Cerna, A. (2013). Bystanders' support of cyberbullied schoolmates. *Journal of Community & Applied Social Psychology*, 23(1), 25–36. doi:10.1002/casp.2135
- Mason, K. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, 45(4), 323–348. doi:10.1002/pits.20301
- McKenna, K. Y. A., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the internet for personality and social psychology. *Personality and Social Psychology Review*, 4(1), 57–75. doi:10.1207/S15327957PSPR0401_6
- McQuade, C. S., Colt, P. J., & Meyer, B. N. (2009). *Cyber bullying: Protecting kids and adults from online bullies*. Westport, CT: Praeger.
- Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007). The relative importance of online victimization in understanding depression, delinquency, and substance use. *Child Maltreatment*, 12(4), 314–324. doi:10.1177/1077559507305996 PMID:17954938
- Mouttapa, M., Valente, T., Gallagher, P., Rohrbach, L. A., & Unger, J. B. (2004). Social network predictor of bullying and victimization. *Adolescence*, 39, 315–335. PMID:15563041
- Olweus, D. (1993). *Bullying at school. What we know and what we can do*. Malden, MA: Blackwell Publishing.
- Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148–169. doi:10.1177/1541204006286288
- Perren, S., Dooley, J., Shaw, T., & Cross, D. (2010). Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents. *Child and Adolescent Psychiatry and Mental Health*, 4(1), 1–10. doi:10.1186/1753-2000-4-28 PMID:21092266

- Pornari, C. D., & Wood, J. (2010). Peer and cyber aggression in secondary school students: The role of moral disengagement, hostile attribution bias, and outcome expectancies. *Aggressive Behavior, 36*(2), 81–94. doi:10.1002/ab.20336 PMID:20035548
- Rideout, V. J., Roberts, D. F., & Foehr, U. G. (2005). *Generation M: Media in the lives of 8-18-year-olds: Executive summary*. Menlo Park, CA: Henry J. Kaiser Family Foundation.
- Rosen, L. D. (2007). *Me, Myspace, and I: Parenting the Net Generation*. New York: Palgrave Macmillan.
- Sahin, M. (2010). Teachers' perceptions of bullying in high schools: A Turkish study. *Social Behavior and Personality, 38*(1), 127–142. doi:10.2224/bp.2010.38.1.127
- Sevcikova, A., Machackova, H., Wright, M. F., Dedkova, L., & Cerna, A. (2015). Social support seeking in relation to parental attachment and peer relationships among victims of cyberbullying. *Australian Journal of Guidance & Counselling, 15*, 1–13. doi:10.1017/jgc.2015.1
- Shapka, J. D., & Law, D. M. (2013). Does one size fit all? Ethnic differences in parenting behaviors and motivations for adolescent engagement in cyberbullying. *Journal of Youth and Adolescence, 42*(5), 723–738. doi:10.1007/10964-013-9928-2 PMID:23479327
- Shariff, S., & Hoff, D. L. (2007). Cyber bullying: Clarifying legal boundaries for school supervision in cyberspace. *International Journal of Cyber Criminology, 1*, 76–118.
- Sijtsema, J. J., Ashwin, R. J., Simona, C. S., & Gina, G. (2014). Friendship selection and influence in bullying and defending. *Effects of moral disengagement. Developmental Psychology, 50*(8), 2093–2104. doi:10.1037/a0037145 PMID:24911569
- Sjurso, I. R., Fandream, H., & Roland, E. (2016). Emotional problems in traditional and cyber victimization. *Journal of School Violence, 15*(1), 114–131. doi:10.1080/15388220.2014.996718
- Smith, P. K., Del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms? In S. Bauman, D. Cross, & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, methodology* (pp. 26–40). New York, NY: Routledge.
- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, and Allied Disciplines, 49*(4), 376–385. doi:10.1111/j.1469-7610.2007.01846.x PMID:18363945
- Sourander, A., Brunstein, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., ... Helenius, H. (2010). Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. *Archives of General Psychiatry, 67*(7), 720–728. doi:10.1001/archgenpsychiatry.2010.79 PMID:20603453
- Stoll, L. C., & Block, R. Jr. (2015). Intersectionality and cyberbullying: A study of cybervictimization in a Midwestern high school. *Computers in Human Behavior, 52*, 387–391. doi:10.1016/j.chb.2015.06.010
- Strohmeier, D., Aoyama, I., Grading, P., & Toda, Y. (2013). Cybervictimization and cyberaggression in Eastern and Western countries: Challenges of constructing a cross-cultural appropriate scale. In S. Bauman, D. Cross, & J. L. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, and methodology* (pp. 202–221). New York: Routledge.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, 7(3), 321–326. doi:10.1089/1094931041291295 PMID:15257832

Tangen, D., & Campbell, M. (2010). Cyberbullying prevention: One primary school's approach. *Australian Journal of Guidance & Counselling*, 20(2), 225–234. doi:10.1375/ajgc.20.2.225

Toledano, S., Werch, B. L., & Wiens, B. A. (2015). Domain-specific self-concept in relation to traditional and cyber peer aggression. *Journal of School Violence*, 14(4), 405–423. doi:10.1080/15388220.2014.935386

Totura, C. M. W., MacKinnon-Lewis, C., Gesten, E. L., Gadd, R., Divine, K. P., Dunham, S., & Kamboukos, D. (2009). Bullying and victimization among boys and girls in middle school: The influence of perceived family and school contexts. *The Journal of Early Adolescence*, 29(4), 571–609. doi:10.1177/0272431608324190

Wade, A., & Beran, T. (2011). Cyberbullying: The new era of bullying. *Canadian Journal of School Psychology*, 26(1), 44–61. doi:10.1177/0829573510396318

Wong, D. S., Chan, H. C. O., & Cheng, C. H. (2014). Cyberbullying perpetration and victimization among adolescents in Hong Kong. *Children and Youth Services Review*, 36, 133–140. doi:10.1016/j.childyouth.2013.11.006

Wright, M. F. (2013). The relationship between young adults' beliefs about anonymity and subsequent cyber aggression. *Cyberpsychology, Behavior, and Social Networking*, 16(12), 858–862. doi:10.1089/cyber.2013.0009 PMID:23849002

Wright, M. F. (2014a). Cyber victimization and perceived stress: Linkages to late adolescents' cyber aggression and psychological functioning. *Youth & Society*.

Wright, M. F. (2014b). Predictors of anonymous cyber aggression: The role of adolescents' beliefs about anonymity, aggression, and the permanency of digital content. *Cyberpsychology, Behavior, and Social Networking*, 17(7), 431–438. doi:10.1089/cyber.2013.0457 PMID:24724731

Wright, M. F. (2014c). Longitudinal investigation of the associations between adolescents' popularity and cyber social behaviors. *Journal of School Violence*, 13(3), 291–314. doi:10.1080/15388220.2013.849201

Wright, M. F. (2015). Cyber victimization and adjustment difficulties: The mediation of Chinese and American adolescents' digital technology usage. *Cyberpsychology (Brno)*, 1(1), 1. Retrieved from <http://cyberpsychology.eu/view.php?cisloclanku=2015051102&article=1>

Wright, M. F. (in press). Adolescents' cyber aggression perpetration and cyber victimization: The longitudinal associations with school functioning. *Social Psychology of Education*.

Wright, M. F., Kamble, S., Lei, K., Li, Z., Aoyama, I., & Shruti, S. (2015). Peer attachment and cyberbullying involvement among Chinese, Indian, and Japanese adolescents. *Societies (Basel, Switzerland)*, 5(2), 339–353. doi:10.3390/soc5020339

Wright, M. F., & Li, Y. (2012). Kicking the digital dog: A longitudinal investigation of young adults' victimization and cyber-displaced aggression. *Cyberpsychology, Behavior, and Social Networking*, 15(9), 448–454. doi:10.1089/cyber.2012.0061 PMID:22974350

Wright, M. F., & Li, Y. (2013a). Normative beliefs about aggression and cyber aggression among young adults: A longitudinal investigation. *Aggressive Behavior*, 39(3), 161–170. doi:10.1002/ab.21470 PMID:23440595

Wright, M. F., & Li, Y. (2013b). The association between cyber victimization and subsequent cyber aggression: The moderating effect of peer rejection. *Journal of Youth and Adolescence*, 42(5), 662–674. doi:10.1007/10964-012-9903-3 PMID:23299177

Ybarra, M. L., Diener-West, M., & Leaf, P. (2007). Examining the overlap in internet harassment and school bullying: Implications for school intervention. *The Journal of Adolescent Health*, 1(6), 42–50. doi:10.1016/j.jadohealth.2007.09.004 PMID:18047944

Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, 45(7), 1308–1316. doi:10.1111/j.1469-7610.2004.00328.x PMID:15335350

Yousef, W. S. M., & Bellamy, A. (2015). The impact of cyberbullying on the self-esteem and academic functioning of Arab American middle and high school students. *Electronic Journal of Research in Educational Psychology*, 23(3), 463–482.

Zhou, Z., Tang, H., Tian, Y., Wei, H., Zhang, F., & Morrison, C. M. (2013). Cyberbullying and its risk factors among Chinese high school students. *School Psychology International*, 34(6), 630–647. doi:10.1177/0143034313479692

ADDITIONAL READING

Bauman, S. (2011). *Cyberbullying: What counselors need to know*. Alexandria, VA: American Counseling Association.

Bauman, S., Cross, D., & Walker, J. (2013). *Principles of cyberbullying research: Definitions, measures, and methodology*. New York, NY: Routledge.

Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Sage Publications.

Li, Q., Cross, D., & Smith, P. K. (2012). *Cyberbullying in the global playground*. Malden, MA: Blackwell Publishing. doi:10.1002/9781119954484

Menesini, E., & Spiel, C. (2012). *Cyberbullying: Development, consequences, risk and protective factors*. New York, NY: Psychology Press.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277–287. doi:10.1016/j.chb.2009.11.014

Wright, M. F. (2016). *A social-ecological approach to cyberbullying*. Hauppauge, NY: NOVA Publisher.

KEY TERMS AND DEFINITIONS

3

Anonymity: The quality of being unknown or unacknowledged.

Anxiety: A mental health disorder which includes symptoms of worry, anxiety, and/or fear that are intense enough to disrupt one's daily activities.

Collectivism: A cultural value that stressed the importance of the group over individual goals and cohesion within social groups.

Cyberbullying: Children's and adolescents' usage of electronic technologies to hostilely and intentionally harass, embarrass, and intimidate others.

Empathy: The ability to understand or feel what another person is experiencing or feeling.

Externalizing Difficulties: Includes children's and adolescents' failure to control their behaviors.

Individualism: The belief that each person is more important than the needs of the whole group or society.

Loneliness: An unpleasant emotional response to isolation or lack of companionship.

Normative Belief: Beliefs about the acceptability and tolerability of a behavior.

Parental Mediation and Monitoring: The strategies that parents use to manage the relationship between their children and media.

Parenting Style: The standard strategies that parents use in their child rearing.

Peer Attachment: The internalization of the knowledge that their peers will be available and responsive.

Peer Contagion: The transmission or transfer of deviant behavior from one adolescent to another.

Provictim Attitudes: The belief that bullying is unacceptable and that defending victims is valuable.

Social Exclusion: The process involving individuals or groups of people block or deny someone from the group.

Traditional Face-to-Face Bullying: The use of strength or influence to intimidate or physically harm someone.

Internet “Death Groups” in the Online Culture

Liudmila Vladimirovna Baeva

 <https://orcid.org/0000-0003-0439-525X>

Astrakhan State University, Russia

INTRODUCTION

Human existence in the space of online / digital / e-culture and information society is becoming more diverse and attractive. The digital culture used to be limited to only leisure, arts, education, and communication; over the last 20 years, it has become an essential part of the digital economy and business, e-government and online services, without which the entire social system would be malfunctioning now. A present-day person, who lives in the Internet era, would regard any gap in the electronic environment as something undermining the very fundamentals of his/her existence. Philosophic, anthropologic, social, and existential issues of the electronic culture and the digital society have become an object of in-depth research over the last two decades; research activities concerning them are becoming increasingly urgent and topical.

Nowadays the developed countries already face the consequences of virtualization of culture and interpersonal communication. Along with improvement of living standards and significant breakthroughs in medicine, electronics, and robotics, there are new deviations related to deformation of relations between a human and the world, changing attitudes to the virtual environment and communication, and increasing human alienation in the real world. The European countries, the USA, Japan, China and Russia already face the phenomenon of “escape from reality” related to the Internet culture (dependent gamers, hikikomori, etc.). They also face an increasing number of teenage and youth suicides, outbreaks of uncontrolled aggression, withdrawal into a virtual world from the real one, and increased dependence on gadgets and online presence in virtual reality; these issues are now regarded as real threats to existence of the present-day society. Virtual communities promoting murders or suicides have become a real hazard for human life and health.

Leading academic and collegiate centers in different countries of the world have been recently dealing in studying of the influence of informatization on different socio-cultural processes. Thus the issues of the development of electronic culture are the subject matter for the scientists in the University of Milan (A. Ronchi, 2009); McLuhan Institute (Virtual Maastricht McLuhan Institute (VMMI), the Netherlands (K.H. Veltman, 2004); studying ethical and anthropological issues of the information space are the subject matter for the researchers in the International Centre for Innovation in Education (ICIE) Karlsruhe, Germany (R. Capurro, 2006); London School of Economics, department of Media and Communication (Great Britain) (L. Haddon, 2004); Centre for Computing and Social Responsibility (De Montfort University, Great Britain) (S. Rogerson, 1998); Center for the Study of the Information Society of the University of Haifa, Israel (D.R. Raban, 2009); ethical, political and legal aspects of informatization are the subject matter for L. Rocci (2012); B. J. Kallenberg (2001), C.L. Chang (2011) and others.

Issues by J. Baudrillard (1993), P. Virilio (1984), B. Heller (2012), M. Heim, (1993), B., Girard, S. Siochru (2003) and P.C. Rivoltella (2008) focused to influence of e-culture (digital culture) to the hu-

DOI: 10.4018/978-1-5225-9715-5.ch045

man values, lifestyle and worldviews. Professor of Harvard University Floridi L. conducted a study on philosophy of information and ethical issues of using information technology (2013). Professor of the London Open University A. Duff a, considered ethical issues of Internet development and addressed the issues of copyright, digital inequality and violation of the right to private life (2008). F. Schäfer (2009), E. Castronova (2005) studied existential issues and risks of the information society and development of cyberculture. These problems were also raised in our earlier studies related to existential-ethical and anthropological aspects of the electronic and media culture development.

Based on the abovementioned research findings and conclusions, let us study “the death groups” operating in the Internet (“Blue Whale”, “Wake Me Up at 4:20”, etc.), which have been attracting much attention in Russian and international social media since 2015, as they provoked teenagers to commit suicide, as well as “the Columbine communities” that promote copycat crimes at educational institutions.

Our research is based on both existential and axiological approaches, as well as on an empirical data analysis (by reviewing Internet communities and their web sites). Our research determines the risk factors and characterizes “the death groups” and “the Columbine communities” as complex social phenomena of the online culture.

History of “Death Groups”

A criminal phenomenon in the digital sphere was emergence of the so-called “death groups”, whose members are forced to commit suicide. Those groups are focused mainly on adolescents, whose minds are not still developed completely, who are susceptible to manipulation. Teenage group members make their choices unconsciously; they are guided by external manipulation and obscure mechanisms that control their will or mind. They are usually driven by a desire to experience something thrilling and extreme, which is due to their disappointment in the real life. In Russia, such online groups began to spread in the social networks in 2015-2016, which has led to a number of investigations, changes in legislation, and introduction of tougher penal measures for driving someone to suicide by doing that via the Internet in particular. Similar communities have also emerged in other countries (including Ukraine, Kazakhstan), although they have not expanded so much.

The “death groups” attracted public attention in Russia in 2015, after Rina Palenkova, a teenage girl from the Siberian city of Ussuriysk, had committed a suicide. She jumped in front of a train on November 22. Just a few minutes before her death, she posted her photo with words of farewell in the most popular social networking service in Russia – VK (VKontakte). Her photo and message quickly became an Internet meme. After Rina’s death, Philipp Lis, who was the administrator of the community named “F57”, who had an intention to gain attention, publicly acknowledged his involvement in her death, as well as in some other teenager suicides. To emphasize his role, he pointed out that there was a direct link between his group and the groups “Sea of Whales” and “Silent House”. There were eight similar groups in the social networks; those groups regarded suicide as a martyrdom, a self-sacrifice that one should glorify. According to some Internet myths, souls of those who committed suicide allegedly went to the “Silent House”. This a meme of online stalking culture denoting the lowest level of the hidden web, a special state of conscience upon reaching which it is impossible to return to the real world, where they could find freedom and peace at the level of digital rebirth. Members of the community were mentally unstable teenagers, and Philipp Lis drove them to suicide by engaging them in a game. The theme of suicide, which traditionally attracts attention of young people of a certain psychological type or in a critical situation, has become popular in social networks. A number of Internet communities began to claim that they control behavior of adolescents and drive them to suicide.

The “death groups” is the name that generally describes online communities that give children assignments in a game form, thereby driving them to suicide day by day. Those communities make their members carry out more and more difficult tasks, from scratching a picture of a whale on their arms (as it is well known, whales are able to commit suicide) to jumping from roofs of high buildings and other forms of suicide. As a result, approximately 130 children perished in Russia in 2015-2016. During this period, there were at least 1,500 groups promoting suicide in VK.

As a result of investigation of 15 children’s and teenagers’ deaths, 21-year-old Phillip Budeykin (aka Lis), who administered eight “death groups”, the most notorious of which was “Blue Whale”, was arrested on November 16, 2016. The investigation was initiated in May 2016, after several Russian mass media had released news about the so-called “death groups” — numerous communities where young people were encouraged to kill themselves. In 2017, Budeykin was found guilty and sentenced to serve a prison term for 3 years and 4 months as per Clause 110 and Part 3 of Clause 30 of the Russian Criminal Code for encouraging people to commit suicide. The investigation is still in progress in a number of Russian regions—Krasnodar, Komi, Bashkortostan, Moscow, Volgograd, Voronezh, Tula, Kemerovo, Novosibirsk, and Omsk. In 2017, the social network VK recorded over 4,000 groups that promoted suicide. According to Anna Kuznetsova, Commissioner for Children’s Rights in the Russian Federation, the number of children suicides in 2016 increased by 57% (compared with 2015). Among European countries, Russia has the largest number of teenage suicides over the recent years (Gareth, 2017).

Similar communities started to appear and gain popularity among teenagers (“F57”, “Wake Me Up at 4:20”, “Sea of Whales”, “Insider”, and “Silent House”). Their primary aim was to glorify death and suicide. The game included both online and offline modes; virtual tasks were to be performed in the real life. For instance, the “Blue Whale” game had a special algorithm of actions for a teenager to follow: 1) a teenager was to make a post on his/her web page hashtagged #I’m in the game; 2) then he/she was assigned to a supervisor who gave him/her tasks and controlled their completion; 3) if any task was not complete, the teenager was threatened that his/her family members would be injured or killed. The tasks were given on a daily basis; there were 50 of them (there is a reference to the book “50 Days before My Suicide” by S. Kramer). The first tasks implied that a teenager had to cut out a picture of a whale on his/her hand; then he/she was to take a picture of himself/herself standing on a roof edge proving that he/she really did that. After that, a teenager had to kill an animal and record a video. Most teenagers dropped out at that point. The last task was “to deliver the world from his/her existence” by committing suicide in that or that form (by jumping from a roof or in front of a train, by hanging, etc.). The average age of the “death groups” members was mainly 10 to 14 years old. To enhance the impact upon them, horrible sounds, screams, psychedelic music, videos of death penalties, and other effects were applied, especially at a particular nighttime (at 4:20 a.m.). The main memes of the “death groups” are a blue whale, a butterfly (living just one day), and a “4:20” inscription.

Many teenagers and children perceive their participation in such groups as extreme entertainment. Like everything that is forbidden and related to mystery and fear, participation in such a community resembles a game for them. Moreover, they regard the tasks that those groups set them as a quest or a mission. This mechanism aims to involve more and more members in those groups. Not all the teenagers perceive the game seriously. However, there are still new victims. The “Blue Whale” game used scenarios that are popular among teenagers in cyber games: a multi-level access system, initiation tasks, obtainment of a particular status, application of symbols and signs. However, it was not a leisure or an entertaining game; it was a destructive psychological technology, which was created by those who are competent in issues of self-destruction.

After the scandalous trial, the teenagers' suicide rate commenced to decrease, and social networks' administrators and volunteers (primarily parents of deceased children) began to ban "death groups".

However, this phenomenon has not been eliminated. Over the last several years, an information war between people who promote suicidal communities and people who oppose them has been taking place in Russia. According to the "Anti-Blue Whale. We Oppose Deaths" community project, the death groups have become increasingly popular since 2017 again; they began to perform their activities in Instagram and Telegram, since their VK pages were banned. After the notorious "Blue Whale", "Whales' Sea", "Wake Me Up at 4:20", and other groups had been banned, new communities that perform similar activities emerged. In 2017 and 2018, their would-be members posted such requests as "I want to play" or "I am looking for a supervisor". Supervisors invite new members after checking their age and making sure that they deal with a teenager or a child. The newly recruited members are requested to make a small payment (50 rubles), and the game begins. Many supervisors are former players who have passed all the game levels, except for the last one, so now they coach others. Those groups often include drug addicts; their supervisors recommend that they should take drugs not to fall asleep. It becomes more and more difficult to locate such supervisors, because they are often former game players.

Viral messages related to the "Run or Die" game, in which children were requested to cross a road in front of moving vehicles, appeared in February 2018. In January 2018, a new game, whose name is "24-Hour Disappearance", emerged; it suggested that children should leave home. This game circulated in VK. According to psychologists, information about the committed suicides spreads like a virus among young people, so it can serve as a catalyst for more and more suicides. Application of such mass mailing techniques in order to attract teenagers' attention to suicide exerts destructive influence. At the same time, we believe that if the threat is obscure and the administrators of those groups act indirectly, only via a chain of associations, in this case the priming effect takes place. It implies application of certain signs and memes, which evoke particular associations in one's mind. In its turn, it results in anxiety and self-destructive tendencies. Hence, the amendments to the Federal Law concerning immediate blocking of "the death groups", which were adopted in Russia in 2018, are a crucial step in order to stop their dissemination and neutralize their fatal impact upon their victims.

Information about the game "Blue Whale Challenge" has spread in a number of countries. Police in the USA, the UK, New Zealand, and Africa warned about its hazards in the media; it also informed students' parents at schools of its destructive nature. In particular, activities performed by "the death groups" are regarded as a reason for an increased percentage of child suicides in India since 2017 (Srivastava, 2017). In 2018, the Indian law enforcement agencies informed teachers that teenagers are profoundly interested in the "Blue Whale" game, as well as in the "Momo" game that was created for WhatsApp; the authorities highly recommended that educators should monitor children's behavior more attentively (Press Trust of India, 05/09/2018).

People who tend to join the "death groups" are exposed to the same risk as totalitarian cults' members, as their conscience is highly susceptible to external manipulation. They are usually prone to depression; they have a weak will and lack social support from their close relatives and friends. Another aggravating factor is that they go through the pubertal period, when people tend to suffer from loneliness and face misunderstandings in their relations with whom they love. A third factor contributing to a deep impact that the "death groups" exert upon their victims is teenagers' tendency to express and feel strong emotions, take risks, and experience something thrilling and risky (Cuss, 2014).

Considering the "death groups", we deal with not only ordinary suicides, but also manipulations that apply certain behavioral blueprints and psychological techniques. In fact, it is a form of hidden violence. Forced suicides, unlike free-will ones, are caused by different motives. By means of destructive

physiological techniques, victims are forced to take a fatal step. Those psychological techniques exploit specific features of adolescence, young people’s interest in death and mysticism, their high sensitivity, susceptibility to abuse and intimidation, tendency to address an adult friend (supervisor) for help and advice, and an extremely strong desire to become an adult.

The psychological factor also contributes to existence of those high-risk groups. Besides the social factor, existential vacuum and shortage of meaningful goals and values, which help a person survive even under the most unfavorable conditions, play an essential role in a young person’s joining a “death group”. The way the modern youth understands the meaning of life proves to relate to their individual manifestation in the Internet, to their personal fulfillment, welfare, entertainments, and extreme experiences that fill their lives with striking moments. Formed by advertisers, the ideology of consumerism, the digital media environment, and virtual communities, those patterns exert a decisive impact upon a young person’s worldview. Neither family and religion, nor culture and education can offer a young person who joined a risk group a positive response to the most acute question of existence: “Is life worth living?” Loss of desire to live and communicate becomes the reason for committing suicides and escaping from the real world into a parallel life. The most widely spread theme among young people in network communities is their disappointment and inability to experience positive emotions. The virtual environment deprived of real emotional bonds makes a lonely person face such existential problems that cannot be resolved where the virtual communication prevails. All this contributes to growth of pessimism, boredom, and apathy, which are definitely background factors of suicide, since life seems to have no purpose or value.

FACTORS AND RISKS

People tending to join “death groups” have a risk like the one that followers have in of totalitarian sects. This type of persons is highly susceptible to external manipulation of their consciousness. They tend to depression, frustration, they have a weak will, they lack social support of friends, positive relationships with parents. Adolescence also increases alienation and rejection of others. And finally, another important factor contributing to children joining the “death groups” is the desire for extreme sensations and risk (Cuss, 2014).

In the case of “death groups” like “Blue whales” we see not only ordinary suicides, but it is a situation with manipulations imposed by behavioral scenarios and the use of certain psychotechnics. In fact, it is a form of hidden violence. Curator of such groups used features of adolescence, interest to death questions, mystery, high sensitivity, susceptibility to abuse and intimidation, a reference point to an adult friend, the desire to be an adult, exceptionally strong. Important role in getting to a risk group caused by existential vacuum, lack of meaningful goals and values that help a person survive even under the most unfavorable conditions. Modern youth’s values focus on personal fulfillment, welfare enjoyment, entertainments and peak experiences that fill the life with striking moments. Family, religion, education can’t offer to youth from a risk group the grounds for a positive answer to the main existential question – “Is life worth living?” The loss of meaning of life and communication becomes a reason of escapism of reality to virtual lives. The most wide-spread topic among teenagers in network communities is disappointment and loss of ability to experience positive emotions. A virtual environment without real emotional bonds leaves a person one on one with existential problems that cannot be solved under conditions of prevalent virtual communication. The weakening of these factors favors growing pessimism, boredom and apathy as a background for suicide as the end of the life that has no sense or value.

Administrators of virtual «death groups» use scenario like virtual games (RPG) for motivation followers pass all the stages. They use the manipulation of behavior and consciousness, based on the characteristics of juvenile psychology, to destroy the boundaries between the game and reality, allowed and forbidden. Curators of groups romanticized death and suicide as an act of freedom under own rules.

Nowadays the electronic environment is not the only foundation for modern communication and unbelievable society integration but also the ground for both conscious and unconscious escape from social reality, new escapism manifestations, refusal from a wish to live in the real world. Virtual “death groups” are the most dangerous escapism manifestation leading to suicide as a complete refusal to live.

The digital environment creates new variants of transform communication and change sociality, existence of human but it one don't give a sense of life. Being in the digital “here and now” is becoming a new personal existential problem for subject. Freedom from reality and its objectivity can lead a human being not only to self-development and creativity but to the highest degree of loneliness and digital autism (Kuss, D.J., Griffiths, M.D., Karila, L., & Billieux, J., 2014). It can also amplify escapism and suicidal ideas typical of borderline cases and conditions.

J. Baudrillard thoroughly explored the essence of the human entry into the virtual culture. He determined the ontologic status of the simulation in terms of the formation of the “hyper-reality”, absorbing and eliminating the reality (Baudrillard, 1994). Discussing the consequences of the virtual hyper reality development, J. Baudrillard asserts that the impetuous development of the virtual will lead to implosion, i.e., blurring of the borders between the real and alternative worlds. Under condition of online culture, the object - subject relations replace subject-object ones when the things, the products created by individuals, start swallowing up their originators, manipulating them, and subordinating them to their functioning.

Real relationship with other people and own status become less important than communication in “second life” (Brey, 1999).. All the choices in virtual reality are made by milder rules, the boundaries between norms and deviations become transparent, as well as truth and lie, good and evil, game and reality. This boundlessness for a digital world is perceived as a norm which has no clear guidelines.

Person's virtual being was initially intended to be a tool, a supplement to his/her real existence; however, as far as different forms of e-communication and media culture are developed, virtual being becomes a terminal value adding “mass” to a real object like a proton. The value shift from a real sphere of the being to a virtual one also indicates changes in human essence, his/her life and environment.

The most dangerous tendencies of developed digital culture lead to the loss of traditional culture and vital world of man which have existed for thousands of years and which are now disappearing under the impact of virtualization of culture. The annihilation of traditional values, models and norms of behavior formed at the level of social groups and communities leads to the change of lifestyle of man molded by new eclectic, informative and open cultural conditions which causes a greater openness and instability of the individual himself.

Serious risks are connected with the transfer of values in virtual worlds, social networks, which complicates the real communication and the capability to solve vital problems, hence develops the destructive way of thinking and self-destructive behavior. The dangerous contents of the suicide groups are the factors that contributes strongly to the self-destructive behavior of the youth. Internet game disorder, loss of real vital emotions caused by perception of oneself and his milieu as virtual world characters can be other reasons of such behavior. Interpersonal communication is being replaced by its virtual imitation, such important spheres of relations such as love and friendship are being ejected also.

Simulation of life in virtual space with the loss of the boundaries of real and game space, normative guidelines of behavior, weakening of real communication, its replacement by virtual forms become factors of existential risk for young people. The most dangerous processes in virtual communication

are associated with deliberate manipulation of consciousness, the extreme forms of which are “death groups”. Their identification and monitoring should be part of the work of law enforcement agencies, volunteers and educators around the world, as this threat has no political boundaries.

ACKNOWLEDGMENT

The study was prepared with grant funding, Russian Foundation for Basic Research (RFBR) grant № 19-29-14007 МК.

REFERENCES

- Baudrillard, J. (1994). *Simulacra and Simulation* (S. F. Glaser, Trans.). Ann Arbor, MI: University of Michigan Press.
- Brey, P. (1999). The Ethics of Representation and Action in Virtual Reality. *Ethics and Information Technology*, 1(1), 5–14. doi:10.1023/A:1010069907461
- Capurro, R. (2006). Towards an Ontological Foundation of Information Ethics. *Ethics and Information Technology*, 8(4), 175–186. Retrieved from <http://www.capurro.de/oxford.html>
- Castells, M. (1997). *The End of the Millennium, the Information Age: Economy, Society and Culture* (Vol. 3). Cambridge, MA: Blackwell.
- Castronova, E. (2008). *Synthetic Worlds*. University of Chicago Press.
- Chang, C. L. (2011). The Effect of an Information Ethics Course on the Information Ethics Values of Students—A Chinese guanxi culture perspective. *Computers in Human Behavior*, 27(5), 2028–2038. doi:10.1016/j.chb.2011.05.010
- Cockton, G. (2004). From quality in Use to Value in the World. In *Proceedings of the CHI'04 Extended Abstracts on Human Factors in Computing Systems (CHI'04)*. New York: ACM Press. 10.1145/985921.986045
- Duff, A. (2008). The Normative Crisis of the Information Society. *Cyberpsychology (Brno)*, 2(1). Retrieved from <http://cyberpsychology.eu/view.php?cisloclanku=2008051201&article=3>
- Gareth, D. (2017). *Social media ‘teen death groups’ encouraging suicides sweep across Russia prompting 57 percent increase in youngsters taking their own lives*. Retrieved February 2018, from <http://www.dailymail.co.uk/news/article-4374978/Social-media-death-groups-prompts-57-rise-suicides.html#ixzz57Rb7E69z>
- Gilbert, R. L., Murphy, N. A., & Ávalos, C. M. (2011, October). Communication Patterns and Satisfaction Levels in Three-Dimensional Versus Real-Life Intimate Relationships. *Cyberpsychology, Behavior, and Social Networking*, 14(10), 585–589. doi:10.1089/cyber.2010.0468 PMID:21381970
- Komsomolskaya Pravda. (2018). “Momo” game in What’s App. Retrieved August 2018, from <https://www.kp.ru/daily/26860/3906471/>
- Kosnik, A. (2016). *Rogue Archives: Digital Cultural Memory and Media Fandom*. MIT Press. doi:10.7551/mitpress/10248.001.0001

Kuss, D. J., Griffiths, M. D., Karila, L., & Billieux, J. (2014). Internet addiction: A systematic review of epidemiological research for the last decade. *Current Pharmaceutical Design*, 20(25), 4026–4052. doi:10.2174/13816128113199990617 PMID:24001297

Miller, V. (2013). *Understanding digital culture*. London: Sage.

Ott, M., & Pozzi, F. (2011). Towards a New Era for Cultural Heritage Education: Discussing the Role of ICT. *Computers in Human Behavior*, 27(4), 1365–1371. doi:10.1016/j.chb.2010.07.031

Press Trust of India. (2018). *Momo Challenge: ICSE association in West Bengal warns schools about 'game', suggests awareness drives for parents and students*. Retrieved November 2018, from <https://www.firstpost.com/india/terrorists-who-killed-bjp-leader-anil-parihar-in-kishtwar-have-been-identified-claims-jammu-and-kashmir-governor-satya-pal-malik-5504271.html>

Raban, D. R. (2009). Self-Presentation and the Value of Information in Q&A Websites. *Journal of the American Society for Information Science and Technology*, 60(12), 2465–2473. doi:10.1002/asi.21188

Rogerson, S. (1998). *Social Values in the Information Society*. FTI Annual Report 1998, Forum of Information Technology, Milan, Italy. Retrieved January 2018, from <http://dehn.slu.edu/courses/fall06/493/rogerson.pdf>

Ronchi, A. M. (2009). *E-Culture*. New York: Springer-Verlag, LLC.

Schäfer, F. (2009). Ludic Philosophy: Subjectivity, choice and virtual death in digital media. *Digital Culture & Education*, 1. Retrieved from http://www.digitalcultureandeducation.com/uncategorized/dce1016_schafer_html

Srivastava, D. (2017). *What the Blue Whale Challenge's popularity tells us about vulnerable teenagers?* Retrieved October 2018, from <https://www.firstpost.com/living/what-the-blue-whale-challenges-popularity-tells-us-about-vulnerable-teenagers-3924181.html>

Turner, R., & Eden, A. H. (2008). The Philosophy of Computer Science. *Journal of Applied Logic*, 6(4), 459–626. doi:10.1016/j.jal.2008.09.006

Verplanken, B., & Holland, R. W. (2002). Motivated Decision Making: Effects of Activation and Self-Centrality of Values on Choices and Behavior. *Journal of Personality and Social Psychology*, 82(3), 434–447. doi:10.1037/0022-3514.82.3.434 PMID:11902626

Zhou, L., Ding, L., & Finin, T. (2011). How is the Semantic Web evolving? A Dynamic Social Network Perspective. *Computers in Human Behavior*, 27(4), 1294–1302. doi:10.1016/j.chb.2010.07.024

Tech That, Bully!

Defeating Cyberbullying With Its Own Weapons

Maria Rosa Miccoli

Idego Psicologia Digitale, Italy

Giulia Gargaglione

Idego Psicologia Digitale, Italy

Simone Barbato

Idego Psicologia Digitale, Italy

Lorenzo Di Natale

Idego Psicologia Digitale, Italy

Valentina Rotelli

Idego Psicologia Digitale, Italy

Valentina Silvestri

University of Milan-Bicocca, Italy

INTRODUCTION

As technology grows, human progression flourishes. Unfortunately, related issues also increase. One of the most worrying and alarming side effect of technology is cyberbullying.

If traditional bullying can be somehow associated with an ancient and instinctual desire to compete with others for survival (Donagan, 2012), cyberbullying is more difficult to frame. Even though both phenomena are a peculiar way for perpetrators to show their superiority, cyberbullying goes further: perpetrators are not just meant to overcome the opponents, their purpose is to psychologically annihilate them.

As Donagan (2012) reports, unlike traditional bullying, cyberbullying allows the offender to mask his or her identity behind a computer. Being anonymous allows perpetrators to hurl abuses and offenses at victims without having to assist to their victim's physical reaction. This "distancing effect" leads offenders to do or say things they probably would have never said or done in presence.

Nowadays, psychology is aware that the increasing diffusion of technology (Fairburn and Patel, 2016) represents a great challenge: researchers with different backgrounds must cooperate to create a virtuous exchange "man-machine". It is fundamental that the foundations of this interaction must be solid and built following specific knowledge to make technologies useful for the human cognitive progress and for people's security (Gamberini, Chittaro, & Paternò, 2012).

DOI: 10.4018/978-1-5225-9715-5.ch046

BACKGROUND

Cyberbullying is defined by Bauman, Underwood and Card (2013) as an extension of traditional bullying that involves the typical behaviors of bullying perpetrated through the use of various technologies, electronic devices in particular (e-mail, instant messaging applications, social media etc.).

Another valuable definition is provided by Belsey (2004). Belsey (2004) defines cyberbullying as a form of violence that “involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal Websites, and defamatory online personal polling websites, to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others”.

Nowadays, cyberbullying is inducing significant socio-cultural problems and psychological disorders, which requires a rapid solution. In recent years, cyberbullying has grown and now it is getting plenty of attention due to the increasingly massive use of digital devices. According to Tokunaga (2010), 97% of young Americans are connected through the Internet, while 20-40% of young people have been victim of online bullying harassment at least once in their lifetime.

Kowalski (2014) argues that cyberbullying entails relevant psychopathological risks: victims report increased depressive symptoms (Jung et al., 2014) and social anxiety; perpetrators are more likely to show aggressive behavior, due to their lack of emotional self-regulation (Kowalski, Limber & McCord, 2018). This unconventional form of bullying towards peers is also linked to suicidal attempt among adolescents (Patchin and Hinduja, 2006). Indeed, some researches showed that certain psychological factors are crucial predictors for both being a cyberbully or a victim. As Alim (2016) reports, low self-esteem is linked to a lack of confidence in one's ability and therefore it is quite easy for a cyberbully to leverage on this to afflict the victim; depression and suicidal ideation are side effects of being a designated victim (Alim, 2016). Cyberbullying not only implies high risks for teen-agers' health (Nixon, 2014), but also substantial economic costs for the families of victims for cleaning up their children online reputation of: legal fees, safety measures, psychological counseling, public relation assistance. In a Reuters post, Amy Tannery (2016) reports that a new insurance policy has been also developed in the United States in order to mitigate the financial cyberbullying consequences.

Before deepening cyberbullying, the differences between bullying and cyberbullying will be object of discussion in order to delineate an accurate overview of the phenomenon.

TRADITIONAL BULLYING VS. CYBERBULLYING

Risks connected to cyberbullying are as damaging as those of traditional bullying. When speaking of virtual environments, the main difference is that bullies can count on further protection factors such as anonymity. As a matter of fact, the possibility of hiding personal identity triggers a *disinhibition effect* leading some kids to say things that typically they would have never said face to face (Suler, 2004). However, some research found that at least 40–50% of cyber victims know the identity of the perpetrator (Kowalski & Limber, 2007; Wolak, Mitchell, & Finkelhor, 2007).

Some people could probably say that the use of technology as a mean of oppression is the only relevant difference between cyberbullying and traditional bullying. Indeed, much has already been written on this topic. This may not be the right place to deepen it, yet a quick *excursus* can help the reader to frame and contextualize the main aspects that make cyberbullying so destructive and blasting.

Actions and Threats

In traditional bullying, peer-directed physical violence is perpetrated through acts of deliberate aggression, including beating, and directs acts of verbal insults and offences (Corcoran et al., 2015; Willard, 2005).

In cyberbullying, cyber-aggression is defined by Grigg (2010) as “intentional harm delivered by the use of electronic means to a person or a group of people irrespective of their age, who perceive(s) such acts as offensive, derogatory, harmful, or unwanted” (p. 152). Cyberbullying conveys a different kind of violence that is psychological and subtle perpetrated using texts, photos, drawings, videos, and audio messages (Willard, 2005). Willard also recognizes 7 types of cyberbullying activity (in Wright et al., 2009):

- **Flaming:** Sending angry, vulgar messages to a person or a party;
- **Harassment:** Sending messages to a person repeatedly;
- **Denigration:** Sending/posting harmful, untrue information;
- **Cyberstalking:** Using threats of harm and intimidation;
- **Impersonation:** Pretending to be another person;
- **Outing or trickery:** Tricking a person into sending embarrassing information;
- **Exclusion:** Excluding someone on purpose.

Place

Traditional bullying is perpetrated in “real world” settings in terms of time and geography (Corcoran et al., 2015). Offences are in a way “restricted” to a physical place (like school).

In cyberbullying, electronic devices know no boundaries of space and time: offences can be put in action at any place at any moment in a repetitive way (Corcoran et al., 2015). Abuse may take place where the victims feel normally safe (home, community centers, places of worship, etc.) aggravating their sense of oppression and powerlessness.

Gender

In traditional bullying, males tend to bully others and be bullied through physical threats and aggressions (Bosworth, Espelage, & Simon, 1999) while girls tend to use psychological violence through a savvy use of relations and communication (Willard, 2005).

In cyberbullying, Tokunaga (2010) reports that research on differences in gender victimization lacks in findings. Few studies found out that females are more often chosen as target of cyberbullies involving psychological torment (Stephenson & Smith, 1989). Some studies highlight that “girls inflict virtual abuse more than boys through instant messaging, online conversations, and e-mails while boys are more likely to make online threats and build websites targeting others”. (Migliore, 2003 in Keith and Martin, 2005; Willard, 2005; Beale & Hall, 2007; Kowalski & Limber, 2007; Li, 2007)

Power

In traditional bullying, power derives mainly from physical prowess and higher social skills: in face to face bullying there is a power imbalance between bullies and their victims (Willard, 2005).

While in traditional bullying power is a pretty clear concept, it is difficult to define it in the cyber world: it could be the ability to stay anonymous, or to hold greater tech skills in order to inflict offences

on a large scale (Corcoran et al., 2015). Willard (2005) reports that online communication could potentially change power balance providing victims with the possibility to retaliate.

Rationalization

Willard (2005) reports that traditional rationalizations made by “face to face” bullies include justification of morally doubtful behaviors made through a shift of responsibility: victims are accountable for making the bully start a certain (bad) behavior (“*He/she started to; he/she told me to; he/she deserves to...*”).

On the contrary, cyberbullies hide themselves behind the perception of invisibility and/or multiple online identities and personalities. They think to have a supposed right of free speech on the Internet. Moreover, they count on the absence of tangible feedback: in this way they reduce the impact of empathy and recognition of harm (Willard, 2005).

Family Dynamics

If compared to other students, bullies and victims are found to perceive their families more negatively regarding problem solving when speaking of traditional bullying (Cenkseven Önder and Yurtal, 2008). Studies in the literature show that parents of bullies have lower levels of problem solving (Loeber, & Dishion, 1984) while showing higher levels of parent conflicts and discordance (Loeber, & Dishion, 1984; Oliver, Oaks, & Hoover, 1994; Olweus, 1993). Accordingly, Willard (2005) found that parents of bullies demonstrate aggressive problem solving, lack of involvement and no limits setting.

Parents of cyberbullies tend to refuse to get involved in their children’s online activity (Willard, 2005). Often, they use the “respect for their children’s privacy” as an excuse for not checking out their kids’ Internet activities: parents do not want to ask for their children keys and password if not strictly necessary. Parents may also hide the responsibility for controlling kids behind some parental control softwares that lead to insufficient security and lack of involvement (Willard, 2005).

Bystanders

In traditional bullying, bystanders assist to acts of violence without helping the victims or ignoring them on purpose. They normally refuse to get involved and justify their inactivity by saying they were just avoiding the conflict. This reaction is often due to moral disengagement (see also Thornberg and Jungert, 2013).

While traditional bystanders have quite a passive role, cyber-bystanders are proactive and somehow crucial in cyber-based abuse: they legitimate the perpetrator by viewing, “sharing” and “liking” the offences (Corcoran et al., 2015).

Listing the differences between traditional bullying and cyberbullying highlight a key point: technology has not to be intended merely as the cause of cyberbullying, but just as a mean of diffusion. Given that, from our point of view, technology is not just where the problem takes place, but it is where the problem can be solved. As for this, different in-use systems to fight and undermine cyberbullying through digital technologies will be the object of next paragraph.

THE ANSWER OF DIGITAL TECHNOLOGIES TO CYBERBULLYING

In this section, three main reasons for which digital technologies should be used to contrast cyberbullying will be described: victims' silence, capability of reaching the most isolated people and security perceived.

Silence is one of the main issues of this phenomenon due to the fact that the target is predominantly young people. Adolescents are often not mature enough to look for the proper solutions and this increases their feelings of loneliness (Şahin, 2012; Olenik-Shemesh, Heiman & Eden, 2012; Brewer & Kerslake, 2015).

As reported by many studies, most cyber victims do not inform adults about what is happening to them (Yilmaz, 2011; Agatston, Kowalski, Limber, 2012). This is a real problem because the main coping strategies for victims of cyberbullying include telling someone, keeping the situation secret, getting revenge or retirement (Nixon, 2014). It is clear that the only response strategy that doesn't compromise social relationships refers to talking with someone (Nixon, 2014).

Moreover, even if victims tell someone what is happening, adults or authorities are rarely chosen as informants. An analysis by Slonje and Smith (2008) illustrates the types of people chosen by the victims in which to confide their cyber persecution: the majority (50%) don't tell anyone, a large group (35,7%) told a friend, a smaller portion (8,9%) told a parent or guardian and the remaining subjects (5,4%) told someone else.

The diffused silence about the phenomenon requires the capability of authorities and psychologists to find out the best instruments to discover cyberbullying situations. Being able to reach individuals who are cut off from their peers can be the first step in fighting these types of events.

It must be noticed that one of the characteristics of cyberbullying is the lack of express and well-known authorities with the role of regulating misbehaviors on the World Wide Web (Tokunaga, 2010). In traditional bullying the regulation of social rules is undertaken by those such as educators or principals in cyberbullying these figures are absent (Holth & Keyes, 2004). For this reason, researchers and authorities must explore the technological and communicational instruments that are firstly able to discover bullying issues and secondly which make children and teen-agers aware of the existence of authorities responsible for regulating social behaviors on the Internet.

The proper use of technologies by the parents themselves could be a great precaution measure from cyberbullying: parents can carry out behaviors to protect their children from dangerous online events (Eastin, Greenberg & Hofschire, 2006; Livingstone, 2007) and/or share technological knowledge with the entire family to create open discussions concerning the proper use of Internet (Mesch, 2009). An analysis by Mesch (2009) conducted on 935 teens (from the age of 12 to 17 years) living in the United States showed that even if participation in online activities remains a risk factor for cyberbullying, educating parents and restricting access to the Internet are effective protection strategies for this type of phenomenon. In addition to parental control tools (e.g. NetNanny, Qustodio, OpenDNS FamilyShield, KidLogger, etc.), some social networks use lists of insults and offensive words to build moderation tools based on keywords (Van Hee, Jacobs, Emmery, Desmet, Lefever, Verhoeven, De Pauw, Daelemans, Hoste, 2018).

FOCUS OF THE ARTICLE

The previous sections explained the different ways in which cyberbullying, today, is a large-scale and multi-faceted phenomenon.

The authors aim to analyze this phenomenon - which takes advantage of new technologies – explaining which technological tools can be used to defeat it and how. This will be done by drawing on different disciplines and perspectives.

SOLUTIONS AND RECOMMENDATIONS

Unfortunately, the aforementioned tools are not enough to defend children from cyberbullies who often use implicit and inconspicuous strategies and language (Van Hee et al., 2018). For this reason, it is necessary to use the technology itself to further the research and to implement complex and self-learning systems which are able to detect these types of occurrences.

The research is already starting to move toward this direction: Van Hee and colleagues (2018) have proposed a machine learning method which uses a linear Support Vector Machine classifier (Cortes and Vapnik, 1995; Chang and Lin, 2011) to recognize “signals” of cyberbullying and build a detecting system for different kinds of cyberbullying and numerous roles involved. This type of system is not language dependent and it is a great example of how using technology can be the most efficient way to detect this type of phenomenon which is characterized by subtle language and multiple strategies.

Along with the aforementioned reasons, it must be remembered that the Internet is still perceived as safe for bullies and victims because it is the place where everyone (even the most isolated people) can find their own dimension given the numerous possibilities it offers. This is the reason why cyberspace itself is considered as the ideal location to deliver interventions built *ad hoc* for each individual facing a cyberbullying situation (Foody, Samara & Carlbring, 2015). Gámez-Guadix, Orue, Smith and Calvete (2013) analyzed a hypothetical temporal relationship between cyberbullying (as victim and as predator) and a problematic use of Internet. A problematic use of internet can be defined as an overwhelming preoccupation with the Internet and an incapability to govern use of the Internet, even when this has negative consequences (Young, 2011).

A longitudinal statistical model demonstrated how victims of cyberbullying show large scale improper use of internet, but this happens after becoming a cyber victim (Gámez-Guadix et al., 2013) as already indicated by other studies (Leung & Lee, 2012). It has already been demonstrated that improper use of internet is perpetuated to reduce feelings of anxiety and isolation, such as negative emotions (Caplan, 2010). This evidence suggests that victims of bullying and cyberbullying improperly use the Internet as a strategy to escape or avoid the negative feelings of victimization (Gámez-Guadix et al., 2013; Foody et al., 2015). Given this type of diffused coping strategy used by cyberbullies, offering interventions to the victims in the place where despite everything they feel safer is the most efficient and calibrated to the target strategy.

After reviewing the main cyberbullying characteristics to which Digital Psychology can be a response the next sections will look at three classes of interventions recently built in this area to address this complex issue. Moreover, these classes of intervention introduce the proposal of intervention which can be seen in the following section.

DIGITAL PSYCHOLOGY AGAINST CYBERBULLYING

Three categories of interventions made in the field of Digital Psychology are the object of this paragraph.

First, it's useful to observe the utility of a project that consists of a platform for adolescent victims of cyberbullying with the function of treatment and prevention (Jacobs, Vollink, Deuhue & Lechner, 2014). Secondly, a brief observation of social networks which already use new technologies to detect and prevent cyberbullying issues will be then discussed. Lastly, how a conversational agent can be used as a simulation of peer support for the victims will be shown (van Der Zwaan, Jonker & Dignum, 2010).

Jacobs and his colleagues (2014) developed a web-based intervention, *Online Pestkoppenstoppen*, with the aim of teaching cyberbullying victims, 12 to 15 years of age, to deal with anxiety and depression. It is a Platform where users can learn strategies of coping and prevention methods. The peculiarity is that in a web environment like this, learning and prevention are done in an interactive way and with the minimization of feelings of shame.

Different studies have shown that teenagers facing cyberbullying use social support as a coping strategy to a lesser extent (Dehue, Bolman & Vollink, 2008; Kowalsky, Limber & Agatston, 2008; Paris, Varjas, Meyers, Cutts, 2012). For this reason, it is necessary to find strategies that have the capacity to involve adolescents in a different way as Jacobs and colleagues (2014) did. With regard to the ways in which different adolescents can be brought in, it is very important to tailor the interventions such as building a suitable web platform (Jacobs et al., 2014).

The project made by Jacobs and colleagues (2014) represents a great starting point for this category because it teaches users efficient coping strategies through three web-based sessions regarding the importance of the awareness of our thoughts and the coping strategies to stop bullying on the web with a final session of feedback about the previous phases and the correct use of the digital tools.

The fact that each suggestion was drawn up for the personal characteristics of the participants is another positive point for the efficacy of the intervention (Jacobs et al., 2014). There are numerous studies that already show the efficacy of tailored interventions to promote changes at health behavior level (Noar, Benac & Harris, 2007; Krebs, Prochaska & Rossi, 2010; Pot, Paulussen, Ruiter, Eekhout, de Melker, Spoelstra & van Keulen, 2017) and teach coping strategies (Bock, Marcus, Pinto & Forsyth, 2001; Williams & French, 2011; Wagner, Duffecy, Penedo, Mohr & Cella, 2017) especially if associated with feedback by the experts (Jacobs et al., 2014).

What social networks are doing to face cyberbullying is of great importance and will now be explored. Facebook, in collaboration with the Yale Center for Emotional Intelligence, has built a prevention platform (*Safety Bullying* available on <https://www.facebook.com/safety/bullying>) against bullying for the different people involved (children and adolescents, parents and teachers) in this type of phenomenon. This platform provides different tips for each type of person involved and offers different examples of dialogue between the implicated people. In 2011, Facebook created a Compassion Team which is formed of researchers from Berkeley and Yale University to improve communications with people who posted improper photos of other people and the results have been positive in terms of taking down the photo or sending a reply to the requests (Anderle, 2016).

Moreover, Google (Perspective) and Instagram are providing machine learning and artificial intelligence tools to recognize the offensive comments and take the necessary precautions.

Particularly, the work that Facebook is perpetuating with its *Safety Bullying* platform is interesting because it's a first attempt to also involve bystanders in this issue. Bastiaensens, Vandebosch, Poels, Van Cleemput, DeSmet and De Bourdeaudhuij (2014) made an analysis of the bystanders' reactions to different situations that showed different types of reactions according to different variables. This study

by Bastiaensens and colleagues (2014) showed that the intentions of helping the victims increased according to the severity of the incidents but instances of joining in bullying is higher when the bullies are the bystanders' friend. Considering these types of social behaviors, precautions made by social networks are necessary to sensitize bystanders and to empower them (Davis and Nixon, 2012).

In conclusion, it is willingness of the authors describing a type of intervention that include the design of a type of embodied conversational agent (ECA) built by van Der Zwaan, Jonker and Dignum (2010). It is a simulation of peer support for cyberbullying victims that communicates in three phases with the user (emotional communication, information gathering and practical advice). Van Der Zwaan and colleagues (2010) define it as a "anti-bullying buddy" which gives child strategies to cope with negative emotions associated with the cyberbullying for facing future similar incidents. It represents a real form of empathy and social support (van Der Zwaan et al., 2010).

Embodied conversational agents can be defined as characters which are generated by computers and they are a simulation of key properties specific of human face-to-face conversation (Provoost, Lau, Ruward & Riper, 2017). This type of tool is being used for mental disorder (Provoost et al., 2017) and concerning the issue of the present article it's an example of how it could provide victims social support through new technologies such as Artificial Intelligence or Virtual Reality environments.

The importance of the perceived social support from peers is fundamental for individuals who are facing a transition (Furman and Buhrmester, 1992; Malecki and Elliot, 1999). Particularly, the importance of perceived social support was proven to be a protective factor against cyberbullying (Holt and Espelage, 2007). In this perspective, a social support simulator (van Der Zwaan et al., 2010) represents a great and controlled opportunity for situations in which real social support is lacking or it's not properly provided.

The three aforementioned categories of interventions are examples of how the scientific research community and social networks are working to face the complex phenomenon of cyberbullying through a proper use of technologies.

The next section is dedicated to the use of a new technology that can operate at an individual level with the creation of controlled environments: Virtual Reality.

FUTURE DIRECTIONS

For the future directions of the research, authors aim to deepen the role that Virtual Reality can have to prevent cyberbullying. By way of explanation of this argument, a deepening of the literature is necessary.

Virtual Reality (VR) is a tool of great potentialities because it integrates a specific communication interface in 3D interactive environment with the collecting of numerous inputs in a unique experience with a high level of similarity to reality (Riva, 2005). Besides, two peculiarities of VR are the capability of creating realism and the possibility to measure this sense of *presence* (Schuemie, van Der Straaten, Krijn & van Der Mast, 2001). This immersion gives users the possibility to have very rich experiences and to easily transfer the learnings of VR situations to the real life.

VR can operate against cyberbullying by capturing the intrinsic characteristics of the phenomenon, to implement correct real-life behavior in safe and protected environments. It allows the creation of realistic virtual environments, with a high level of control (Witmer and Singer, 1998) and security (Sahoo, Mohapatra & Lath, 2010). The VR responds to the main needs of the cyberbullying protagonists: feeling comfortable in virtual environments and the need for security.

On the other hand, it is necessary to look at the fact that bullies could use virtual reality to mistreat the victims, for example using multiplayer VR games. In 2016, the COFACE (Confederation of Family

Organization in the European Union) published a paper outlining the dangers of using VR in the most advanced video games, suggesting useful tips to mitigate their misuse.

In awareness of this danger, the authors aim to explain how virtual reality can be used as a “cure” for cyberbullying behavior, not as a tool in the bullies’ hands.

VIRTUAL REALITY AGAINST CYBERBULLYING

The VR instruments are used above all in the field of psychological intervention, especially for Post-traumatic Stress Disorder (PTSD) treatment (Rizzo, 2006). However, the scenario is currently changing, psychologists are realizing advantages and benefits of this therapy in several sectors. For example, virtual reality can be used to increase people’s empathy because of specific situations. In the past, ad hoc contexts have been developed by researchers to modulate different roles of power (Raybourn, 1999) or to recreate war environments, capable of shaking even the most convinced of war rightness (see the so called ProjectSyria).

Regarding cyberbullying and the importance of immersion for treatment, it can be useful to make a brief analysis of *FearNot!* (Fun with Empathic Agents to Reach Novel Outcomes in Teaching). *Fear!Not* is an anti-bullying intervention for children from 8 to 12 years of age (Hall, Paiva & Aylett (2009). It is not specific for cyberbullying but it can be used as structure for future more specific interventions. It was being developed for 7 years, before being included within the VICTEC (Virtual ICT with Empathic Characters) project and then in eCIRCUS (Education through Characters with emotional Intelligence and Role-playing Capabilities that Understand Social Interaction) (Hall et al., 2009). The tool provides an episodic virtual drama in which the user personifies the “invisible friend” of the character that is the victim of bullying. So, the user has the task of giving help with advice that influences the behavior of the victim and gives rise to different scenarios (Hall et al., 2009). Moreover, the results of a longitudinal evaluation showed a positive impact of *Fear!Not* on bullying in terms of information and cognizance (Sapouna, Wolke, Vannini, Watson, Woods, Schneider, Enz, Hall, Paiva & Aylett, 2010).

The great opportunity given by this type of intervention is that it provides supportive and secure learnings through experiences, moreover there is the possibility to distribute this type of intervention in the schools, to entire classrooms (Hall et al., 2009). Although, for the purposes of this article it’s important to highlight another reason for the success of the *Fear!Not* application: the social relationship created by the user with the synthetic character (Louchart, Aylett, Hall, Woods & Paiva, 2006). The realism and the social relationship created by this type of project are positive signals for the potentialities that the VR could provide to cyberbullying.

In conclusion, the authors of this article propose VR as a future instrument of response to cyberbullying for three specific reasons: VR applications can be used by numerous realities, they have the capability to deliver more efficient training about emotions and the fact that adults must be involved into this type of training can improve trust toward adults. In support of this argument, below are some examples of these conceptualizations.

An example of how VR can be wide ranging is the project built by the Harmony Labs (available on Harmony Labs.org) which presents a curriculum formed of six lessons of three-five minute VR experiences. The brevity and the availability of this type of project shows how VR can have a great impact even with brief training sessions that can be transferred to real-life situations.

The Amanda Project is a VR training tool about emotions associated with cyberbullying which was created by a group of Greek engineers for the Microsoft Imagine Cup (2016). It can be used by the us-

ers through an app and virtual reality glasses, making them live the situation of bullying both from the bystander and the victim perspectives. Then, the physical feedback changes the experiences. The creators say that the data can be used to improve awareness, empathy and self-confidence to help people answer to situations of bullying properly.

In relation to the importance of involving adults in cyberbullying phenomenon to increase their reliability for children, a prototype of training for teachers to identify bullying could be a great opportunity to create more positive societies and has already shown positive results (Stavroulia, Ruiz, Harisiou, Manouchou, Georgiou, Sella & Lanitis, 2016).

Given these results with different types of project that use VR it is necessary to further the research this direction to build specific contents and guidelines with respect to the Virtual Reality characteristics. It should be noted that VR could be the answer to cyberbullying as an instrument that can be used by qualified psychologists who are able to contextualize the emotions associated with the virtual environment compared to the real one.

To further the role of cyberbullying in different directions, being aware of different contexts in which this can be present and of the dedicated funds that are necessary. In the end, a glance at future scenarios influenced by other new technologies will be discussed.

Cyberbullying doesn't only affect children and teen-agers: nowadays, young adults and adults are also impacted by this phenomenon. A widespread use of social media is present for people of any age as can be seen by the Internet usage reports of Wearesocial and Hootsuite, published in 2018 (Lombardi, 2018): these statistics show, for example, that the major use of Facebook is by people from 18-34 years old and followed by 35-44 years olds, while those aged 13-17 years old and 46-54 years old show similar statistics.

The fact that the cyberbullying continues into adult age demonstrates a serious problem because adults better know how to operate without being charged. On the other hand, the victims can see damage not only for themselves but also for their families and their social and work life.

Cyberbullying among adults can be divided into three main categories: trolling, cyber harassment and flaming. Trolling occurs when someone creates dissension on web communities posting provocative and unrelated messages with the purpose of creating outrage among the users (Gammon, 2014). Cyber harassment is a sequence of web activities carried out by one or a group of people with the aim of provoking emotional distress in a specific victim (Bocij, 2004). Flaming is the use of messages (mostly e-mails) which show enmity, aggressiveness, and coercion in the communication with the other person (Turnage, 2008).

A study of Kircaburun and colleagues (2018) showed that there are commonalities between cyberbullies of different ages (problematic social media use and cyberbullying perpetration) and this is an additional signal that the population needs major sensibilization and research concerning this issue.

Given the positive characteristics of new technologies and of virtual reality environments, it is necessary for the institutions to start investing in creating VR environments and videogame funds. This investment must be done both in terms of treatment and prevention and sensibilization. Schools should be a context from which to start but placing funds also for adult training is of equal importance. As aforementioned, some examples of these types of positive VR environments, videogames and online communities already exist but they still are not widespread enough. A firm action by the institutions and through research is necessary. Involving technologies and new technologies in this type of work is necessary for many different reasons such as: the reproduction of realistic and involving environments, other than the clarification of the proper use of those technologies.

The progress of new technologies is a reality and a significant opportunity for the world. This must not be the opportunity for a growth in cyberbullying, as much as a way for positive development for

humanity and for detecting misuse of technologies (cf. Google Perspective, Instagram). Regarding this, Megan Meier Foundation is a positive sign of how artificial intelligence can be used to fight cyberbullying (Meier, 2018): a foundation created by a mother's victim of cyberbullying can be capable to recognize the benefit of technologies. IBM Watson technologies are being used since 2016 from Megan Meier Foundation and Identity Guard to categorize millions of messages through natural language processing (NLP) and natural language classifiers (NLC).

In conclusion, the purpose of future research must consist of clarifying the underlying psychological causes of cyberbullying and of using technology to defeat this phenomenon.

CONCLUSION

The pervasive diffusion of new technologies within new generations can be a threat or an opportunity. This different prospect relies on the research and the quality of knowledge that we will offer to new generations. The only certainty is that stopping technology is not an option nor a solution.

Once it is understood that bullying and cyberbullying are distinct phenomenon, to further research it is important to understand the distinction between them at both a theoretical and practical level. Building cohesive theories regarding cyberbullying will make researchers better able to understand this phenomenon and design well-targeted projects (Tokunaga, 2010).

Digital technologies and digital psychology have been providing different types of professional solutions in response to characteristics of cyberbullying such as silence, isolation and lack of safety perceived by the people involved. After a brief review of the psychological intervention that used platforms with tailor-made advices (Jacobs et al., 2014), social networks which provide platforms and artificial intelligence tools for prevention and the possibilities offered by an ECA in this field (van Der Zwaan et al., 2010) it is possible to have a greater understanding of how psychology and other disciplines are cooperating to build efficient solutions for cyberbullying with the available technology.

Virtual Reality (VR) can be used as treatment for all of the protagonists involved in cyberbullying (bullies, victims, bystanders, educators and parents) because it creates virtual environments with high level of realism but also control with the possibility of replicability by professional adults. This can be instrumental in increasing the trust of children and adolescents toward adults in order to build constructive relationships.

In conclusion, increasing VR research regarding cyberbullying could be the answer in terms of improving the scientific method and making projects *ad hoc* for different types of targets.

REFERENCES

- Agatston, P., Kowalski, R., & Limber, S. (2012). Youth views on cyberbullying. In J. W. Patchin & S. Hinduja (Eds.), *Cyberbullying Prevention and Response: Expert Perspectives* (pp. 55–71). New York, NY: Routledge.
- Alim, S. (2016). Cyberbullying in the World of Teenagers and Social Media: A Literature Review. *International Journal of Cyber Behavior, Psychology and Learning*, 6(2), 68–95. doi:10.4018/IJCB-PL.2016040105
- Amanda Project. (n.d.). *AMANDA Project - Virtual Reality Anti-Bullying App*. Author.

Anderle, M. (2016). Making a More Empathetic Facebook - The company's compassion department researches ways to make confrontations and breakups a little easier online. *The Atlantic – Technology*.

Bastiaensens, S., Vandebosch, H., Poels, K., Van Cleemput, K., DeSmet, A., & De Bourdeaudhuij, I. (2014). Cyberbullying on social network sites. An experimental study into bystanders' behavioural intentions to help the victim or reinforce the bully. *Computer. Human Behavior*, 31, 259–271. doi:10.1016/j.chb.2013.10.036

Bauman, S., Underwood, M.K., & Card, N.A (2013). Definitions: Another perspective and a proposal for beginning with cyberaggression. *Principles of cyberbullying research: Definitions, measures, and methodology*, 41-46.

Beale, A., & Hall, K. (2007). Cyberbullying: What school administrators (and parents) can do. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, 81(1), 8–12. doi:10.3200/TCHS.81.1.8-12

Belsey, B. (2004). *Cyberbullying.ca*. Retrieved July 31, 2004, from Web site: www.cyberbullying.ca

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family*. Westport, CT: Praeger.

Bock, B. C., Marcus, B. H., Pinto, B. M., & Forsyth, L. H. (2001). Maintenance of physical activity following an individualized motivationally tailored intervention. *Annals of Behavioral Medicine*, 23(2), 79–87. doi:10.1207/S15324796ABM2302_2 PMID:11394558

Bosworth, K., Espelage, D., & Simon, T. (1999). Factors associated with bullying behavior among early adolescents. *The Journal of Early Adolescence*, 19(3), 341–362. doi:10.1177/0272431699019003003

Brewer, G., & Kerslake, J. (2015). Cyberbullying, self-esteem, empathy and loneliness. *Computers in Human Behavior*, 48, 255–260. doi:10.1016/j.chb.2015.01.073

Caplan, S. E. (2010). Theory and measurement of generalized problematic Internet use: A two-step approach. *Computers in Human Behavior*, 26(5), 1089–1097. doi:10.1016/j.chb.2010.03.012

Cenkseven Önder, F., & Yurtal, F. (2008). An Investigation of the Family Characteristics of Bullies, Victims, and Positively Behaving Adolescents. *Educational Sciences: Theory and Practice*, 8(3), 821–832.

Chang, C.C., & Lin, C.J. (2011). LIBSVM: A Library for Support Vector Machines. *ACM Transactions on Intelligent Systems and Technology*, 2(3).

COFACE – Confederation of Family Organisations in the European Union (2016). COFACE Paper – Cyberbullying, New dimensions through virtual environments and other emerging platforms and trends. *Coface-EU*.

Corcoran, L., Mc Guckin, C., & Prentice, G. (2015). Cyberbullying or Cyber Aggression?: A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression. *Societies (Basel, Switzerland)*, 5(2), 245–255. doi:10.3390/oc5020245

Cortes, C., & Vapnik, V. (1995). Support-Vector Networks. *Machine Learning*, 20(3), 273–297. doi:10.1007/BF00994018

Davis, S., & Nixon, Cl. (2012). Empowering bystanders. In J. Patchin & S. Hinduja (Eds.), *Cyberbullying Prevention and Response: Expert Perspectives* (pp. 93–113). New York, NY: Routledge.

- Dehue, F., Bolman, C., & Völlink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. *Cyberpsychology & Behavior*, 11(2), 217–223. doi:10.1089/cpb.2007.0008 PMID:18422417
- Donegan, R. (2012). Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis. *The Elon Journal of Undergraduate Research in Communications*, 3(1), 33–42.
- Eastin, M., Greenberg, B., & Hofschire, L. (2006). Parenting the Internet. *Journal of Communication*, 56(3), 486–504. doi:10.1111/j.1460-2466.2006.00297.x
- Facebook - Security Centre. (n.d.). *Safety Bullying*. Retrieved December 10, 2018, from Facebook.org
- Fairburn, C. G., & Patel, V. (2016). The impact of digital technology on psychological treatments and their dissemination. *Behaviour Research and Therapy*, 88, 19–25. doi:10.1016/j.brat.2016.08.012 PMID:28110672
- Foody, M., Samara, M., & Carlbring, P. (2015). A review of cyberbullying and suggestions for online psychological therapy. *Internet Interventions*, 2(3), 235–242. doi:10.1016/j.invent.2015.05.002
- Furman, W., & Buhrmester, D. (1992). Age and sex differences in perceptions of networks of personal relationships. *Child Development*, 63(1), 103–115. doi:10.2307/1130905 PMID:1551320
- Gamberini, L., Chittaro, L., & Paternò, F. (Eds.). (2012). *Human-Computer Interaction. I fondamenti dell'interazione tra persone e tecnologie*. London: Pearson.
- Gámez-Guadix, M., Orue, I., Smith, P. K., & Calvete, E. (2013). Longitudinal and reciprocal relations of cyberbullying with depression, substance use, and problematic internet use among adolescents. *The Journal of Adolescent Health*, 53(4), 446–452. doi:10.1016/j.jadohealth.2013.03.030 PMID:23721758
- Gammon, A. (2014). *Over a quarter of Americans have made malicious online comments*. YouGov.
- George, M. J., & Odgers, C. L. (2015). Seven Fears and the Science of How Mobile Technologies May Be Influencing Adolescents in the Digital Age. *Perspectives on Psychological Science*, 10(6), 832–851. doi:10.1177/1745691615596788 PMID:26581738
- Grigg, D. W. (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. *Australian Journal of Guidance & Counselling*, 20(2), 143–156. doi:10.1375/ajgc.20.2.143
- Hall, L., Aylett, R., & Paiva, A. (2009). FearNot!: providing children with strategies to cope with bullying. *Conference: Interaction Design and Children, Proceedings of the 8th International Conference on Interaction Design and Children, IDC 2009*.
- Harmony Labs (2017). *STAND UP – Virtual Reality to active bystanders against bullying Curriculum Guide*. Retrieved December 9, 2018, from Harmony Labs.org
- Holt, M., & Keyes, M. (2004). Teachers' attitudes toward bullying. In D. Espelage & S. Swearer (Eds.), *Bullying in American schools: A social-ecological perspective on prevention and intervention* (pp. 121–139). Mahwah, NJ: Erlbaum.
- Holt, M. K., & Espelage, D. L. (2007). Perceived Social Support among Bullies, Victims, and Bully-Victims. *Journal of Youth and Adolescence*, 36, 984–994. doi:10.1007/10964-006-9153-3

- Jacobs, N., Vollink, T., Dehue, F., & Lechner, L. (2014). Online Pestkoppenstoppen: Systematic and theory-based development of a web-based tailored intervention for adolescent cyberbully victims to combat and prevent cyberbullying. *BMC Public Health*, 14(1), 396. doi:10.1186/1471-2458-14-396 PMID:24758264
- Jung, Y., Leventhal, B., Shin Kim, Y., Park, T. W., Lee, S., Lee, M., ... Park, J. (2014). Cyberbullying, Problematic Internet Use, and Psychopathologic Symptoms among Korean Youth. [English.]. *Yonsei Medical Journal*, 55(3), 826–830. doi:10.3349/ymj.2014.55.3.826 PMID:24719154
- Keith, S., & Martin, M. E. (2005). Cyber-Bullying: Creating a Culture of Respect in a Cyber World. *Reclaiming Children and Youth*, 13(4), 224–228.
- Kidlogger. (n.d.). *Kidlogger - website*. Retrieved December 10, 2018, from Kidlogger.net
- Kircaburun, K., Kokkinos, C. M., Demetrovics, Z., Király, O., Griffiths, M. D., & Çolak, T. (2018). Problematic Online Behaviors among Adolescents and Emerging Adults: Associations between Cyberbullying Perpetration, Problematic Social Media Use, and Psychosocial Factors. *International Journal of Mental Health and Addiction*. doi:10.1007/11469-018-9894-8
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. doi:10.1037/a0035618 PMID:24512111
- Kowalski, R. M., & Limber, P. (2007). Electronic bullying among middle school students. *The Journal of Adolescent Health*, 41(6), S22–S30. doi:10.1016/j.jadohealth.2007.08.017 PMID:18047942
- Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2008). *CyberBullying: Bullying in the digital age*. Malden, MA: Blackwell Publishing.
- Kowalski, R. M., Limber, S. P., & McCord, A. (2018). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*.
- Krebs, P., Prochaska, J. O., & Rossi, J. S. (2010). A meta-analysis of computer-tailored interventions for health behavior change. *Preventive Medicine*, 51(3–4), 214–221. doi:10.1016/j.ypmed.2010.06.004 PMID:20558196
- Leung, L., & Lee, P. S. N. (2012). The influences of information literacy, internet addiction and parenting styles on internet risks. *New Media & Society*, 14(1), 117–136. doi:10.1177/1461444811410406
- Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, 23(4), 1777–1791. doi:10.1016/j.chb.2005.10.005
- Livingstone, S. (2007). Strategies of parental regulation in the media– rich home. *Computers in Human Behavior*, 23(2), 920–941. doi:10.1016/j.chb.2005.08.002
- Loeber, R., & Dishion, T. J. (1984). Boys who fight at home and school: Family conditions influencing cross-setting consistency. *Journal of Consulting and Clinical Psychology*, 52(5), 759–768. doi:10.1037/0022-006X.52.5.759 PMID:6501661
- Lombardi, A. (2018). Digital in 2018 report: gli utenti internet nel mondo superano i 4 miliardi. In Italia sono più di 43 milioni. We are social.

- Louchart, S., Aylett, R., Hall, L., Woods, S. & Paiva, A. (2006). FearNot! developing social immersion in the VICTEC and ECIRCUS projects. *Semantic Scholar*.
- Malecki, C. K., & Elliott, S. N. (1999). Adolescents' ratings of perceived social support and its importance: Validation of the Student Social Support Scale. *Psychology in the Schools*, 36(6), 473–483. doi:10.1002/(SICI)1520-6807(199911)36:6<473::AID-PITS3>3.0.CO;2-0
- Meier, T. (2018). AI technology helps protect teens from cyberbullying. *IBM blog*.
- Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *CyberPsychological Behavior*, 12(4), 387–393. doi:10.1089/cpb.2009.0068 PMID:19630583
- Migliore, D. (2003). *Bullies torment victims with technology*. Retrieved December 9, 2018, from Az-prevention.org
- Net Nanny. (n.d.). *Net Nanny website*. Retrieved December 12, 2018 from <https://www.netnanny.com/>
- Nixon, C. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, 5, 143–158. doi:10.2147/AHMT.S36456 PMID:25177157
- Noar, S. M., Benac, C. N., & Harris, M. S. (2007). Does Tailoring Matter? Meta-Analytic Review of Tailored Print Health Behavior Change Interventions. *Psychological Bulletin*, 133(4), 673–693. doi:10.1037/0033-2909.133.4.673 PMID:17592961
- Olenik-Shemesh, D., Heiman, T., & Eden, S. (2012). Cyberbullying victimisation in adolescence: Relationships with loneliness and depressive mood. *Emotional & Behavioural Difficulties*, 17(3-4), 361–374. doi:10.1080/13632752.2012.704227
- Oliver, R., Oaks, I. N., & Hoover, J. H. (1994). Family issues and interventions in bully and victim relationships. *The School Counselor*, 41, 199–202.
- Olweus, D. (1993). *Bullying at school*. Cambridge: Blackwell.
- OpenDNS. (n.d.). *Open DNS Family - website*. Retrieved December 10, 2018, from [Opendns.com](https://www.opendns.com/family/)
- Parris, L., Varjas, K., Meyers, J., & Cutts, H. (2012). High School Students' Perceptions of Coping With Cyberbullying. *Youth & Society*, 44(2), 284–306. doi:10.1177/0044118X11398881
- Patchin, J. W., & Hinduja, S. (2006). Bullies Move Beyond The Schoolyard: A Preliminary Look At Cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148–169. doi:10.1177/1541204006286288
- Pot, M., Paulussen, T. G., Ruiter, R. A., Eekhout, I., de Melker, H. E., Spoelstra, M. E., & Van Keulen, H. M. (2017). Effectiveness of a Web-Based Tailored Intervention With Virtual Assistants Promoting the Acceptability of HPV Vaccination Among Mothers of Invited Girls: Randomized Controlled Trial. *Journal of Medical Internet Research*, 19(9), e312. doi:10.2196/jmir.7449 PMID:28877862
- Project Syria (n.d.). *Project Syria_docubase*. Retrieved on December 10, 2018, from [Docubase.mit.edu](https://docubase.mit.edu/)
- Provoost, S., Lau, H. M., Ruward, J., & Riper, H. (2017). Embodied Conversational Agents in Clinical Psychology: A Scoping Review. *Journal of Medical Internet Research*, 19(5), e151. doi:10.2196/jmir.6553 PMID:28487267
- Qustodio. (n.d.). *Qustodio website*. Retrieved December 10, 2018 from [Qustodio.com](https://www.qustodio.com/)

- Raybourn, E. M. (1999). *An intercultural computer-based multi-user simulation supporting participant exploration of identity and power in a text-based networked virtual reality: Domecity(TM)MOO*. ProQuest Information & Learning.
- Riva, G. (2005). Virtual Reality in Psychotherapy [Review]. *Cyberpsychology & Behavior*, 8(3), 220–230. doi:10.1089/cpb.2005.8.220 PMID:15971972
- Rizzo, A., Pair, J., Graap, K., Manson, B., McNerney, P. J., Wiederhold, B., & Spira, J. (2006). *A Virtual Reality Exposure Therapy Application for Iraq War Military Personnel with Post Traumatic Stress Disorder: From Training to Toy to Treatment*. In *Novel Approaches to the Diagnosis and Treatment of Posttraumatic Stress Disorder* (pp. 235–250). Washington, DC: IOS Press.
- Şahin, M. (2012). The relationship between the cyberbullying/cybervictimization and loneliness among adolescents. *Children and Youth Services Review*, 34(4), 834–837. doi:10.1016/j.childyouth.2012.01.010
- Sahoo, J., Mohapatra, S., & Lath, R. (2010). Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues. *2010 Second International Conference on Computer and Network Technology*. 10.1109/ICCNT.2010.49
- Sapouna, M., Wolke, D., Vannini, N., Watson, S., Woods, S., Schneider, W., ... Aylett, R. (2010). Virtual Learning Intervention to Reduce Bullying Victimization in Primary School: A Controlled Trial. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, 51(1), 104–112. doi:10.1111/j.1469-7610.2009.02137.x PMID:19703096
- Schuemie, M. J., van der Straaten, P., Krijn, M., & van der Mast, C. A. P. G. (2001). Research on Presence in Virtual Reality: A Survey. *Cyberpsychology & Behavior*, 4(2), 183–201. doi:10.1089/109493101300117884 PMID:11710246
- Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, 49(2), 147–154. doi:10.1111/j.1467-9450.2007.00611.x PMID:18352984
- Stavroulia, K. E., Harisiou, A. R., Manouchou, E., Georgiou, K., Sella, F., & Lanitis, A. (2016). A 3D Virtual Environment for Training Teachers to Identify Bullying. *Proceedings of the 18th Mediterranean Electrotechnical Conference MELECON 2016*. 10.1109/MELCON.2016.7495417
- Stephenson, P., & Smith, D. (1989). Bullying in the junior school. In D. P. Tattum & D. A. Lane (Eds.), *Bullying in schools* (pp. 45–48). Stoke-on-Trent, UK: Trentham Books.
- Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, 7(3).
- Tannery, A. (2016). *Your Money: Cyber bullying delivers a punch to consumer wallets*. Reuters.
- Thornberg, R., & Jungert, T. (2013). Bystander behavior in bullying situations: Basic moral sensitivity, moral disengagement and defender self-efficacy. *Journal of Adolescence*, 36(3), 475–483. doi:10.1016/j.adolescence.2013.02.003 PMID:23522703
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277–287. doi:10.1016/j.chb.2009.11.014

Van der Zwaan, J., Jonker, C.M., & Dignum, V. (2010). Simulating Peer Support for Victims of Cyberbullying. *New Phytologist*.

Van Hee, C., Jacobs, G., Emmery, C., Desmet, B., & Lefever, E., Verhoeven, B., ... & Hoste, V. (2018). Automatic detection of cyberbullying in social media text. *PLoS One*, 1–22. doi:10.1371/journal.pone.0203794 PMID:30296299

Wagner, L. I., Duffecy, J., Penedo, F., Mohr, D. C., & Cella, D. (2017). Coping strategies tailored to the management of fear of recurrence and adaptation for E-health delivery: The FoRtitude intervention: Managing Fear of Recurrence. *Cancer*, 123(6), 906–910. doi:10.1002/cncr.30602 PMID:28207157

Willard, N. (2005). *Cyberbullying and Cyberthreats*. Center for Safe and Responsible Use of the Internet.

Williams, S. L., & French, D. P. (2011). What are the most effective intervention techniques for changing physical activity self-efficacy and physical activity behaviour—And are they the same? *Health Education Research*, 26(2), 308–322. doi:10.1093/her/cyr005 PMID:21321008

Witmer, B. G., & Singer, M. J. (1998). Measuring presence in virtual environments: A presence questionnaire. *Presence (Cambridge, Mass.)*, 7(3), 225–240. doi:10.1162/105474698565686

Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *The Journal of Adolescent Health*, 41(6), S51–S58. doi:10.1016/j.jadohealth.2007.08.019 PMID:18047945

Wright, V. H., Burnham, J. J., Inman, C. T., & Ogorchock, H. N. (2009). Cyberbullying: Using Virtual Scenarios to Educate and Raise Awareness. *Journal of Computing in Teacher Education*, 26(1), 35–41.

Yilmaz, H. (2011). Cyberbullying in Turkish middle schools: An exploratory study. *School Psychology International*, 32(6), 645–654. doi:10.1177/0143034311410262

Young, K. S. (2011). Clinical assessment of Internet-addicted clients. In K. S. Young & C. N. de Abreu (Eds.), *Internet addiction: A handbook and guide to evaluation and treatment* (pp. 19–34). Hoboken, NJ: John Wiley & Sons Inc.

ADDITIONAL READING

Aboujaoude, E., Savage, M. W., Starcevic, V., & Salame, W. O. (2015). Cyberbullying: Review of an Old Problem Gone Viral. *The Journal of Adolescent Health*, 57(1), 10–18. doi:10.1016/j.jadohealth.2015.04.011 PMID:26095405

Bauman, S., Cross, D., & Walker, J. (Eds.). (2013). *Routledge monographs in mental health. Principles of cyberbullying research: Definitions, measures, and methodology*. New York, NY, US: Routledge/Taylor & Francis Group.

Patchin, J. W. (Ed.). (2011). *Cyberbullying Prevention and Response: Expert Perspectives*. London, UK: Routledge.

Samara, M., Burbidge, V., El Asam, A., Foody, M., Smith, P. K., & Morsi, H. (2017). Bullying and Cyberbullying: Their Legal Status and Use in Psychological Assessment. *International Journal of Environmental Research and Public Health*, 14(12), 1449. doi:10.3390/ijerph14121449 PMID:29186780

Suler, J. R. (2015). *Psychology of the Digital Age: Humans become electric*. Cambridge: Cambridge University Press.

Völlink, T., Dehue, F., & Mc Guckin, C. (2015). *Cyberbullying: from theory to Intervention*. London, UK: Routledge. doi:10.4324/9781315680354

KEY TERMS AND DEFINITIONS

Artificial Intelligence: A multidisciplinary field of research and engineering which studies the human functions that can be emulated by different types of machines.

Bullying: Arrogant attitude of people who oppress their peers through acts of physical and verbal violence. It is diffused mostly in scholar and juvenile contexts.

Cyberbullying: Attitude of overcoming from people that use informatic and web communication to denigrate their peers. It can be extended beyond physical contexts given the lack of boundaries which characterizes the world wide web.

Digital Psychology: It is a multidisciplinary (Behavioral Economics, Psychology, Digital Communication, and Information Technology) approach to psychology which integrates the study of human beings with the research on new technologies.

Embodied Conversational Agent: Characters which are generated by informatic tools and they show properties which are specific of face to face human communication.

Machine Learning: A method of data analysis based on setting automatic learning in technological tools to create analytical systems which are able to detect complex data.

Peer Support: A situational process in which respect and support principles characterize the relationships involving people with common experiences.

Virtual Reality: A virtual environment that simulates reality in which human being can be immersed through tools like glasses and visors. Depending upon different tools, the user can receive and respond to different stimuli.

Cyberbullying in the Workplace

Shalini Ramdeo

The University of the West Indies, St. Augustine, Trinidad and Tobago

Riann Singh

The University of the West Indies, St. Augustine, Trinidad and Tobago

INTRODUCTION

Technology has become the most valuable means to communicate within the contemporary workplace. The reliance on technology is increasing as it shapes the success of modern firms. Emails, messenger, cellular phones, and social media use have extended the interconnectedness among employees beyond the traditional 'brick and mortar' business environment. The advent of the internet has created a new communication tool that has, in many ways, positively revolutionized the interconnectedness of societies and business operations around the globe. As of March 2019, there is an estimated four billion, three hundred and eighty-three million internet users worldwide (Internet World Stats, 2019). In this technological age, however, there is the blurring of boundaries between personal space and workspace as the internet is a potential threat for cyber abuse, and the proliferation of the workplace stressor of cyberbullying. With the internet and modern communication devices, new forms of harassing behaviours have emerged where the target is subjected to online abusive behaviour even after leaving the workplace. Using technology to communicate may be described as a 'double-edged sword' where the increased reliance and dependence for high tech communication decreases the courteous interactions among persons. The erosive effect on interpersonal exchanges can give rise to workplace cyberbullying: an escalating process in which an employee is subjected to perceived psychological abuse recurring over a period of time where the perpetrator uses some form of technology.

For the past thirty years, organizational researchers have become increasingly interested in the dark side of management and employee behaviours, with extensive research being conducted on offline workplace bullying (henceforth referred to as traditional bullying). The increasing interest in this phenomenon has considerably advanced understanding in a relatively short space of time (Nielsen & Einarsen, 2018). Feeling trapped, frustrated, threatened, verbally abused, ignored, isolated, and mentally hurt are all common descriptors used by workers in explaining their employment situations and can be summated as 'domestic violence at work, where the abuser is on the payroll'. The issue of workplace cyberbullying is gaining increasing attention as workplace bullying is no longer confined to the traditional face-to-face work environment but has evolved with the information and communications technology (ICT) revolution. There is the alteration of the social rules that govern the workplace with the co-occurrence of traditional bullying and cyberbullying. Cyberbullying is not restrained by time, tools, or location, as 'work' is no longer a well-defined activity with sharp boundaries. The blurring of boundaries of work, technology, social media, and mobile platforms are modifying the workplace landscape. From a human resources perspective, it is therefore imperative to consider the working context within which cyberbullying occurs.

The objectives of this chapter are to:

DOI: 10.4018/978-1-5225-9715-5.ch047

- Describe the key elements of cyberbullying.
- Explain the difference between traditional bullying and cyberbullying.
- Highlight the main consequences of workplace cyberbullying on the target and on the organization.
- Suggest practical approaches organizations can adopt to prevent and address cyberbullying at work.
- Identify areas for future research on workplace cyberbullying.

BACKGROUND

The workplace has drastically been altered where employees are able to work remotely and connect with colleagues around the world. This interconnectedness is increasing the susceptibility of employees to online abusive interpersonal behaviours referred to as cyber abuse. These behaviours include cyber stalking, cyber bullying, sexual solicitation, and exposure to phonographic material (Mishna, Cook, Saini, Wu, & MacFadden, 2011). One form of cyber abuse in the workplace is ‘cyberbullying’ or ‘cyber-harassment’, by superiors, co-workers, and subordinates. Cyberbullying incorporates the use of a technological form of communication as the means through which a person is harassed, threatened, or abused. Research on cyberbullying and its consequences have focused on school children and adolescents, while the effects on adults in the workplace are now attracting the attention of scholars.

Workplace cyberbullying discussions have been generating research interests among researchers and practitioners for over the past decade, with pioneering studies exploring its conceptualization, prevalence, and consequences. While initial research on cyberbullying emerged among children (Mishna et al., 2011) there is increasing interest of cyberbullying in the workplace setting as it crosses the barrier between work and home. Scandinavian researchers first introduced the concept of ‘mobbing’ in the workplace by extending the view of children being bullied in the playground at schools to include bullying among organizational employees (Leyman 1990). Traditional bullying is a toxic event which violates the fundamental rights of workers as they are subjected to degrading and dehumanising behaviours at the hands of their perpetrator(s).

Traditional Bullying

Exposure to workplace aggression has been conceptualized by various labels such as incivility, victimization, workplace psychological harassment, social undermining, emotional abuse, mobbing, bullying, and abusive supervision. Workplace bullying is defined as “an escalating process in which one or more employees are subjected to negative psychological and physical abuse recurring over an extended period of time (usually 6 months or more), where the target is reduced to a psychologically inferior state and it creates a hostile work environment to those exposed” (Ramdeo, 2017). This form of psychological violence creates an emotionally corrosive work environment as employees struggle to determine whether bullying will continue and how it will affect their job. Traditional bullying is a form of workplace aggression which focuses on perpetrators and targets within the organization. It is necessary to consider the unique aspects of workplace bullying and workplace cyberbullying for policy development and effective management as concise differentiations would allow targets to identify and determine the nature of the behaviours. Although the literature is sparse on workplace cyberbullying, it can be concluded that engaging in these acts of aggression are motivated primarily by the intent to inflict harm and fear.

There is growing agreement among researchers regarding the noteworthy features that define workplace bullying. Firstly, the psychological imbalance that, depending on the degree of exposure, impedes the target's normal functioning. Secondly, the source of bullying, that is, the perpetrator, is someone within the organization, for instance, a supervisor, co-worker, subordinate, or group of workers. The bullying behaviours range along a continuum from subtle to extreme. Thirdly, there is the time element. For behaviour to be considered bullying there is persistent recurrence over an extended period. The perpetrator may use tactics directed to the individual and/or to the individuals work, that is, person-related bullying and/or work-related bullying (Glasø, Nielsen, & Einarsen, 2009). Person-related bullying consists of behaviours such as humiliation or ridicule in front of others, spreading malicious rumours and gossip, making insulting or offensive remarks, constant criticism, intentionally ignoring someone, direct criticism, and physical threats. Work-related bullying consists of behaviours such as excessive monitoring of work, ignoring views and opinions, assigning meaningless tasks, withholding information which can affect a worker's performance, setting unreasonable or impossible deadlines, unmanageable workloads, misuse of power or supervision (for instance, intentionally blocking promotion and/or training opportunities).

Research findings have categorized workplace antecedents or determinants at the levels of the environment, the organization, the situation, the team/group, and the person (Mathisen, Øgaard, & Einarsen, 2012). Not only is workplace bullying linked to job-related and person-related attitudes and behaviours, but also health and well-being consequences (Nielsen & Einarsen, 2012). The meta-analytic review findings by Nielsen and Einarsen (2012) identified and classified the consequences can be classified into three categories (1) job related – job satisfaction, organizational commitment, and turnover intent; (2) health-related outcomes ranging from mental health problems, physical health problems, somatization, post-traumatic stress, burnout, strain, and core self-effectiveness; and (3) behavioural outcomes – performance, and absenteeism. Furthermore, prevention (Duffy, 2009) and coping (Oade, 2009) strategies have been proposed. On the one hand, the promotion of workplace anti-bullying policies as a deterrent has also been advanced. On the other hand, the bully can deny claims being made by the target, claiming that such behaviours were for the advancement of the organization, further increasing the subjectivity surrounding bullying incidents.

A number of pre-conditions exist that triggers an individual to direct bullying actions and behaviours towards others. These include diminutive or no consequences for exhibiting such behaviours, dissatisfaction with the work environment, the power imbalance between the perpetrator and the target, and the personality of the perpetrator. Supervisory bullying (referred to as 'abusive supervision') research was championed by Tepper (2000) and is one of the most common forms of traditional bullying. The lack of status, power, or a formal process to retaliate intensifies the vulnerability of targets when the perpetrator is a supervisor.

With the increasing availability, use, and reliance on electronic technology, deepening understanding of cyberbullying and its implications for organizations should be a priority. Workplace cyberbullying involves the use of technology to bully an organizational employee. Cyberbullying, also known as electronic bullying or online social cruelty, includes the infliction of repeated and intentional harm directed towards another (Mishna et al., 2011). There are various terms that have emerged to describe this workplace phenomenon such as cyber aggression, that is, perceptions of aggression by the target (Weatherbee, 2006), and cyber incivility, that is, violations of the norms of mutual respect in the workplace (Lim & Teo, 2009). Drawing on the theoretical and empirical understandings of workplace bullying, the unique aspects of cyberbullying are explored.

FOCUS OF THE ARTICLE

3

What is Workplace Cyberbullying? The Nature and Dynamics of Cyberbullying

Through cyberspace, negative acts can include online threats, electronic harassment, cyber flashing, and electronic aggression (Farley et al. 2015). A consensus by researchers is yet to be established on whether such acts are repetitive or if it is a one-time occurrence to be classified as cyber bullying. In the work setting, the increasing use of email, text messaging, instant messaging service, social media, and phone conversations are drastically altering the communication process. The use of electronic bulletin, messaging boards, and the implementation of 360-degree performance appraisal platforms often allows employees to post anonymously, providing an avenue for virtual abuse, and more specifically, workplace cyberbullying. Furthermore, the trapped feeling experienced by the victim is intensified with the constant access via electronic devices. It is increasingly challenging as the target is unable to escape the cyberbully when at home and is unable to replenish their coping strategies. Hence, there is a new vulnerability for the victim; a disempowering effect. The victim is unable to psychologically detach from the negative acts being experienced and the violation of their dignity is intensified as compared to traditional bullying.

In establishing a workable and theoretically sound definition of workplace cyberbullying, various definitions have been proposed (Coyne et al., 2017; D'Cruz & Noronha, 2017; Langos, 2012; Vranjes, Baillien, Vandebosch, & Erreygers, 2017). These definitions include certain key elements: inappropriate and unwanted acts of hostility, intimidation, aggression and harassment with the use of ICT to carry out the bullying (for instance via email, website, cell phone, social media); a single or repeated event with the intent to harm another individual (the victim) or group of individuals; the bully can be direct (that is, in communicating with the target) or indirect (that is, posting content to forums, and on social media); the bullying is related to the work context; the persistence and intensity of the behaviours increases over time. Therefore, cyberbullying can be direct or indirect, where the perpetrator uses electronic means to taunt, harass or intimidate the target by communication via messages, pictures, and webpages to target their peers.

There are many different forms of cyberbullying tactics used by perpetrators. Some of the most common forms are as follows:

- *Harassment* is the act where malicious and offensive messages are repeatedly sent to an individual or group by the cyberbully. One form of harassment is cyberstalking where the bully makes continuous threats and sends inappropriate messages, which can manifest into real world physical harassment.
- *Flaming* is the act of posting or sending offensive messages, referred to as ‘flares’, over the internet. This usually involves an online fight where the exchange is via email, forum postings, or instant messaging. Harsh language, profanity, and images are sent to the victim by the cyberbully.
- *Exclusion* is the act where the target is intentionally left out from online/cellular phone chat groups and sites. Malicious comments are made by members of the group about the person that has been singled out. In the workplace, this may include employee chat groups and e-mail groups.
- *Outing* is the act of disseminating private and personal information, videos, and/or pictures about someone over the internet without their consent. The intent is to embarrass or publicly humiliate the target and the person is ‘outed’ when this occurs. In the workplace setting, this may include sharing information about a co-worker from their social media account with other employees who may not be a part of his/her contact listing.

- *Masquerading* is the act where a fake identity is created by the cyberbully to anonymously harass the target. Further, the cyberbully may impersonate another through masquerading to send the malicious messages to the target.
- *Denigration* is the act where an individual is criticized in a derogatory manner by the cyberbully. The intent is to defame someone's character.

Computer-mediated communication is frequently used in the business setting where misunderstandings between the sender and receiver are more likely to occur with online communication. A growing problem in the workplace is the increasing interpersonal hostility when communicating via emails. The underlying tone used to communicate is subject to misinterpretation, triggering negative work attitudes and behaviours by the recipient. Immediate clarification and feedback may be lacking due to the medium of online communication chosen. For instance, the use and intonations in the wording of emails may be perceived as offensive by the recipient since there is a lack of social cues and direct feedback. The reduced social cues or misinterpretation of emotions may explain the low empathy in online communication. Hence, the perpetrator is less aware of the target's reactions, thereby reducing the empathy towards the target and increasing the aggressive nature of the acts.

Many of the tools used by bullies to carry out cyberattacks are not exclusively available only at the workplace. Further complicating this issue is the use of company cellular phones and computers after work hours, blurring the personal boundaries of workers and increasing the difficulty to enforce codes of conduct (West, Foster, Levin, Edmison, & Robibero, 2014). Organisations. Organizations also rely heavily on social media platforms as a marketing tool to promote their products, services, and business. The use of social media tools such as Facebook Business, Twitter, and Instagram implicate the establishment of boundaries and rules on its use and pose a potential avenue for cyberbullying.

Cyberbully and Targets at Work

Cyberbullying can occur downwards, that is, by supervisor to subordinate, horizontally, that is, among co-workers, or upward, that is, subordinate to supervisor. With cyberbullying, the bully can even be a stranger within the organisation (Cruz & Noronha, 2017). Any member of the organisation is susceptible to cyberbullying. In differentiating the target and victim of cyberbullying, the target is an employee who is exposed to persistent cyberbullying behaviours. Based on self-classification, a victim is an employee who identifies as such due to the self-perception of powerlessness.

Traditional Workplace Bullying and Workplace Cyberbullying: Are they Different?

To date, there remains a lack of consensus on the conceptualization and definition of workplace cyberbullying. Earlier conceptualizations of cyberbullying have proposed that it is a form of bullying using technology as an electronic extension (Li, 2007; Privitera & Campbell, 2009). More recently, researchers have suggested that workplace cyberbullying is a distinct concept from traditional bullying (Coyne et al., 2017; Vranjes, Baillien, Vandebosch, & Erreygers, 2017). Workplace cyberbullying shares the same characteristics of traditional bullying where the negative behaviour is repeated over a period of time, and the victim is reduced to a psychologically inferior state. With cyberbullying, however, the repetition may be dependent on the technology and the features of the published content, and not limited to the

behavioural repetition of only the perpetrator, that is, direct and indirect cyberbullying (Langos 2012). The following explores some of the notable distinguishing characteristics of workplace cyberbullying.

Firstly, one key difference between traditional bullying and cyberbullying is *anonymity*. Anonymous cyberbullying can occur as a perpetrator can create a fake email or social media profiles with pseudonyms to disguise their identity. There is a greater detachment when communicating online due to the anonymity of the cyberbully. It can be argued that with traditional bullying, the bully can be identified, and the victim is able to lodge a formal complaint to the necessary organizational agents. With cyberbullying, there is a lack of restraint on what is being said about the victim. It is even more difficult for a formal complaint to be made and the organization to intervene as the victim may be unable to identify the cyberbully. Additionally, the cyberbully does not see the face of the target, thereby not understanding the full extent of the consequences of their actions and taking full responsibility, referred to as the *disinhibition effect*. The ease with which fake social media accounts can be created may allow for anonymous cyberbullying outside work hours.

Secondly, there is a *wider audience* who may be privy to the negative acts being directed to the victim than with traditional bullying. Therefore, the humiliation experienced by the cyber victim is more severe as there is the potential to spread to a limitless audience and persons may unknowingly become co-accomplices by viewing and sharing material about the victim. Social media posts and pictures can be shared without the consent of the individual being targeted.

Thirdly, digital content has a *permanent quality* where it is almost impossible to remove or delete content. Digital content can be downloaded, saved, and stored both online and offline allowing it to be retrieved at any time. Therefore, the victim is faced with the challenge of having shared material permanently remain in cyberspace which can further contribute to the psychological distress of the victim. A single incident can linger, becoming widespread and is an ongoing humiliation for the victim. Furthermore, future employers may also have access to such material when conducting background checks on job applicants.

Fourthly, in stimulating the victim's action, the *personal power* of the victim is diminished with workplace cyberbullying. With traditional bullying, the imbalance of power is associated with the perpetrator's physical and psychological power in the real world. However, with cyberbullying, it is not only limited to the features of the perpetrator, but the 'power of technology' and may be based on the lack of power of the target, rather than the power possessed by the perpetrator (Dooley, Pyzalski, & Cross, 2009). While the victim or target in traditional bullying has the power to leave the organization and end the bullying experience, with cyberbullying this may not be so. The feeling of helplessness can have far reaching implications on the psychological imbalance imposed on the victim. These features have led researchers to argue that cyberbullying has a stronger psychological impact than traditional bullying as there is the ongoing humiliation resulting from being abused online and the potential repercussions for the victim's career and reputation.

Fifthly, with cyberbullying the victim can use the *digital evidence* to report the bullying incidents and for the organizational agent to deal with the reported case. Using the phone caller identifiers, call records, text messages, emails, IP addresses, SIM cards, and website posts have been found to be useful as tangible proof for the target and employers. This available proof act as a shield for the victims and allow them to protect themselves (Cruz & Noronha, 2017). However, with cyberbullying, there is a higher probability that the bully would be more vigilant in concealing his/her identity. When the bully is anonymous then it is challenging for the victim to identify the bully. Further contributing to the under-reporting of cases, organizations are failing to develop and implement cyberbullying policies to

objectively address reported cases of this phenomenon. The lack of interventions to deter cyber abuse in the workplace is enabling such incidents to proliferate.

The Antecedents of Cyberbullying at Work

Communication through digital devices in the workplace is becoming more prevalent, further increasing the possibility for cyberbullying behaviour. Empirical evidence on the antecedents of workplace cyberbullying is relatively sparse. Consistent with research on cyberbullying among adolescents and traditional bullying, stressor evoked emotions of fear and sadness were found to predict exposure to workplace cyberbullying. Further, these mechanisms were significant explanatory reasonings for the relationship between work stressors and exposure to workplace cyberbullying (Vranjes, Baillien, Vandebosch, Erreygers, & De Witte, 2018). Therefore, workers who are sad and fearful are more vulnerable to being targeted by someone in the organization using cyberbullying tactics.

The Implications of Cyberbullying at Work

The technological advancements are expanding at an increasing rate with organizations trailing behind in their attempts to develop and implement codes of conduct to manage cyberbullying behaviours. Added to this is the paucity of research on the impact of cyberbullying in the workplace. While the impact of workplace cyberbullying is not widely studied and understood, extensive research has been conducted on the consequences of traditional bullying on the target/victim and organization.

When false allegations are made about an employee in a public platform, there is the ongoing humiliation and distress experienced. There is the potential for the victim's reputation and career to be adversely affected. Bullying has direct and indirect repercussions for an organization, its reputation, and the potential for negative publicity. When enacted on the internet, the implications for the firm is far-reaching as the scope of harm by a cyberbully can have an outward spiralling dynamic that transcends the internal organizational boundaries. When an employee is being targeted in public forums, reference can be made to the organization which is visible to potential customers, potential investors, and potential employees.

Health-Related Implications of Cyberbullying

Research has consistently shown that workers who are bullied are at a higher risk of negative psychological problems (for instance posttraumatic stress disorder), physical problems (for instance physical abuse, fatigue, muscular complications), physiological problems (for instance diminished self-esteem, emotional exhaustion, shameful feeling, and neuroticism), and psychosomatic problems (for instance sleeplessness and chronic depression). The health-related outcomes of cyberbullying have predominantly been explored from the adolescent's mental health perspective. Some of these effects include increased risk for mental health issues, depression, anxiety, stress, social difficulties, aggression, decreased self-esteem, delinquency, substance abuse, rule-breaking behaviour, and suicidality (Nixon 2014). The reactions to cyberbullying may depend on the form of cyberbullying experienced by the target where adolescents who were victimized via a computer (for instance email, online posts, graphics) experienced greater harm than adolescents victimized via a phone (for instance phone calls, text messaging) (Raskauskas & Stoltz, 2007). Based on the similarities in the health-related effects on targets of both traditional workplace bullying and cyberbullying among adolescents, workplace cyberbullying is expected to have severe implications on the health and well-being of the targeted employee.

Work-Related Implications of Cyberbullying

From the organization's perspective, productivity can be affected as the victims spend more time worrying about incidents when they occur and the likely future interactions with the perpetrator. Some studies have identified work-related implications of workplace cyberbullying. For instance, a study conducted by Lim and Teo (2009) found that female supervisors engaged in passive cyber incivility and male supervisors engaged in active forms of cyber incivility. Their findings also revealed that there was a negative relationship between cyber incivility and employees' job satisfaction and organizational commitment. Interestingly, employees who experienced cyber incivility engaged in deviant behaviour against their organization or were more likely to quit their jobs. In another study conducted by Coyne et al. (2017), the researchers found that those exposed to cyberbullying, when compared to traditional bullying, display a stronger negative relationship with job satisfaction. They concluded that cyberbullying may have more severe outcomes than traditional bullying due to the differences in the strength of the relationship. Muhonen et al. (2017) found that the relationship between cyberbullying behaviour and health, well-being, work engagement, and intention to quit can be mediated by the social organizational climate. Furthermore, there was a stronger indirect effect of cyberbullying behaviour to health, well-being, work engagement, and intention to quit than direct relationships. Stemming from the consistency in the findings, these studies suggest that victims experience lower job satisfaction and higher turnover intentions.

SOLUTIONS AND RECOMMENDATIONS

This new workplace hazard requires systematic efforts towards formulating awareness, prevention, and intervention strategies. The failure to systematically address cyberbullying activities can escalate where intra-relationships are disrupted and eventually evolve into a dysfunctional organization as victims may retaliate by engaging in deviant behaviours as well. There is the increasing need for cyberbullying interventions as proactive approaches should be given priority to effectively resolve such incidents. Organizations need to communicate that it takes cyberbullying seriously and such behaviours will not be tolerated. Specifically tailored interventions are necessary beyond those adopted for traditional bullying. Given the scope and permanence of workplace cyberbullying, the following recommendations are advanced to manage and address cyberbullying:

Internal policies: Organizations should develop a formal policy after consultation with stakeholder groups such as employees, and trade unions. Having a well-organized response can restore the confidence of employees when they recognize that grievances will be handled in due process. In developing an internal policy, the document should entail certain key aspects: a specific definition of cyberbullying; a list of the types of workplace cyberbullying (employees can label their experiences); a detailed grievance process (guidelines in making a formal complaint, the agent to investigate the complaint, the process of investigation, the report submitted upon completing the investigation). Redress mechanisms should be enforced, to be effective in curtailing workplace cyberbullying.

Communication: The cyberbullying policy should be communicated to all staff. A zero-tolerance approach should be communicated throughout the organization to deter cyberbullying behaviours where the bully is dealt with in an expeditious manner. The consequences for violations should be outlined and enforced. Formal statements should be issued to all employees on how the cyberbully was punished to enforce the zero-tolerance approach and to dispel rumours that may be circulating throughout the organizational grapevine.

Mediation between the parties involved: When an employer receives a complaint, it should be addressed in a prompt and thorough manner. In instance where the perceived cyberbully did not realise that the behaviour was unacceptable, the matter can be resolved through a meeting with the two parties that is facilitated by a designated organizational agent. The facilitator can determine if the matter should proceed to a formal complaint being made and disciplinary action taken or if the perpetrator recognises that the behaviour is unacceptable, apologizes, and is committed to changing their ways.

Counselling: The organization should offer professional counselling services to assist victims with the psychological trauma that they may experience. This should be coupled with stress management intervention and coping strategies that can be incorporated into their employee wellness programme.

Training: Sensitivity training on workplace cyberbullying and communicating through the internet should be conducted. Employees will have more information, gain knowledge, and establish a consensus regarding netiquette, acceptable behaviour in electronic communication and the tone of messages sent. Organizations should adopt a proactive approach and communicate with employees on how they can report instances of cyberbullying. This should include the appropriate use of ICT at work; maintain professional boundaries, and privacy settings. Additionally, self-help literature and educational material should be made available to all employees. This should contain approaches to deal with the emotional effects of workplace cyberbullying.

Bystanders: The role and importance of bystanders as key agents in workplace bullying intervention is gaining attention. With cyberbullying, bystanders would play a critical role in deterring bullying by training employees to detect and report incidents. By fostering a supportive organizational culture, witnesses would be willing to come forward to support the claims being made by co-workers. Therefore, organizations must ensure that there are transparent reporting procedures.

Awareness at a National Level: As countries around the world seek to empower their workers and protect them against workplace bullying, current national laws and legislation should be amended to include workplace cyberbullying. Further, to increase awareness and sensitise the public, communication media such as newspaper articles, radio/television programmes, and social media can be effective tools. Trade union involvement to disseminate information to its members can also be a medium to increase awareness of workers.

FUTURE RESEARCH DIRECTIONS

Workplace cyberbullying is an emerging issue that is proliferating at an alarming rate. In order to curtail its occurrence, there is the increasing need to deepen understanding of this phenomenon. Given the current debate on the conceptualization of workplace cyberbullying, further probing is necessary to consider the unique aspects for policy development and effective management. From a legal and organizational perspective, concise differentiations would allow the target to identify and determine the nature of the behaviours.

Future research should explore the implications of the direction, repetition, and form used by the cyberbully. The intensity of the psychological, physical, emotional, and physiological effects on the victim may be shaped by the tactics used by the cyberbully. Therefore, the effects may vary when the cyberbully engages in direct or indirect cyberbullying behaviours, the frequency of the acts, and the use of a computer or a cellular phone. Further, the relationship between cyberbullying, its causes and its consequences are difficult to differentiate. To address this causality dilemma, researchers should apply longitudinal research designs when exploring the antecedents and consequences.

CONCLUSION

In conclusion, workplace cyberbullying is not a trivial issue as it is even more complicated than traditional bullying. There is the critical need for continued research as this area is at its embryotic stage with many unexplored areas as the theoretical discourse regarding this phenomenon is limited. While this phenomenon is grouped as workplace aggression, understanding its unique features and the implications for workers, organizations, and society is necessary with the ICT revolution. As communication through digital devices and social media in the workplace proliferates, there is a danger that cyberbullying behaviour also might become more rampant. Practical interventions need to be developed and implemented to curtail workplace cyberbullying from becoming embedded into the cultures of organizations.

REFERENCES

- Coyne, I., Farley, S., Axtell, C., Sprigg, C., Best, L., & Kwok, O. (2017). Understanding the Relationship Between Experiencing Workplace Cyberbullying, Employee Mental Strain and Job Satisfaction: A Dysempowerment Approach. *International Journal of Human Resource Management*, 28(7), 945–972. doi:10.1080/09585192.2015.1116454
- Cruz, P. D., & Noronha, E. (2017). Workplace cyberbullying : Insights into an emergent phenomenon. In K. Chillas, Briken, M. Krzywdzinski, & A. Marks (Eds.), *The new digital workplace: How new technologies revolutionise work* (pp. 112–131). London: Palgrave.
- Dooley, J. J., Pyzalski, J., & Cross, D. (2009). Cyberbullying Versus Face-to-Face Bullying A Theoretical and Conceptual Review. *The Journal of Psychology*, 217(4), 182–188. doi:10.1027/0044-3409.217.4.182
- Duffy, M. (2009). Preventing Workplace Mobbing and Bullying with Effective Organizational Consultation, Policies, and Legislation. *Consulting Psychology Journal: Practice and Research*, 61(3), 242–262. doi:10.1037/a0016578
- Farley, S., Coyne, I., Axtell, C., & Subramanian, G. (2015). Exploring the Impact of Cyberbullying on Trainee Doctors. *Medical Education*, 49(4), 436–443. doi:10.1111/medu.12666 PMID:25800304
- Forssell, R. (2016). Exploring cyberbullying and face-to-face bullying in working life – prevalence, targets and expressions. *Computers in Human Behavior*, 58, 454–460. doi:10.1016/j.chb.2016.01.003
- Glasø, L., Nielsen, M. B., & Einarsen, S. (2009). Interpersonal Problems Among Perpetrators and Targets of Workplace Bullying. *Journal of Applied Social Psychology*, 39(6), 1316–1333. doi:10.1111/j.1559-1816.2009.00483.x
- Internet World Stats. (2019). *Internet Usage Statistics*. Accessed on June 16, 2019. <https://www.internetworldstats.com/stats.htm>
- Langos, C. (2012). Cyberbullying: The Challenge to Define. *Cyberpsychology, Behavior, and Social Networking*, 15(6), 285–289. doi:10.1089/cyber.2011.0588 PMID:22703033
- Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, 23(4), 1777–1791. doi:10.1016/j.chb.2005.10.005

- Lim, V. K. G., & Teo, T. S. H. (2009). Mind your E-manners : Impact of cyber incivility on employees ' work attitude and behavior. *Information & Management*, 46(8), 419–425. doi:10.1016/j.im.2009.06.006
- Mathisen, G. E., Øgaard, T., & Einarsen, S. (2012). Individual and situational antecedents of workplace victimization. *International Journal of Manpower*, 33(5), 539–555. doi:10.1108/01437721211253182
- Mishna, F., Cook, C., Saini, M., Wu, M. J., & MacFadden, R. (2011). Interventions to prevent and reduce cyber abuse of youth: A systematic review. *Research on Social Work Practice*, 21(1), 5–14. doi:10.1177/1049731509351988
- Muhonen, T., Jönsson, S., & Bäckström, M. (2017). Consequences of cyberbullying behaviour in working life The mediating roles of social support and social organizational climate. *International Journal of Workplace Health Management*, 10(5), 376–390. doi:10.1108/IJWHM-10-2016-0075 PMID:29721038
- Nielsen, M. B., & Einarsen, S. (2012). Outcomes of exposure to workplace bullying: A meta-analytic review. *Work and Stress*, 26(4), 309–332. doi:10.1080/02678373.2012.734709 PMID:23236220
- Nielsen, M. B., & Einarsen, S. V. (2018). What we know, what we do not know, and what we should and could have known about workplace bullying: An overview of the literature and agenda for future research. *Aggression and Violent Behavior*, 42(July), 71–83. doi:10.1016/j.avb.2018.06.007
- Nixon, C. L. (2014). *Current perspectives : the impact of cyberbullying on adolescent health*. Academic Press.
- Oade, A. (2009). *Managing Workplace Bullying*. Palgrave MacMillan. doi:10.1057/9780230249165
- Privitera, C., & Campbell, M. A. (2009). Cyberbullying: The New Face of Workplace Bullying? *Cyberpsychology & Behavior*, 12(4), 395–400. doi:10.1089/cpb.2009.0025 PMID:19594381
- Ramdeo, S. (2017). *Exposure to workplace bullying: The moderated-mediation effects of personal and contextual factors on work-related outcomes in Trinidad and Tobago* (Unpublished doctoral dissertation). The University of the West Indies, St Augustine, Trinidad.
- Raskauskas, J., & Stoltz, A. D. (2007). *Involvement in Traditional and Electronic Bullying Among Adolescents*. doi:10.1037/0012-1649.43.3.564
- Tepper, B. J. (2000). Consequences of Abusive Supervision. *Academy of Management Journal*, 43(2), 178–190.
- Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2017). The dark side of working online : Towards a definition and an Emotion Reaction model of workplace cyberbullying. *Computers in Human Behavior*, 69, 324–334. doi:10.1016/j.chb.2016.12.055
- Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2018). When workplace bullying goes online: Construction and validation of the Inventory of Cyberbullying Acts at Work (ICA-W). *European Journal of Work and Organizational Psychology*, 27(1), 28–39. doi:10.1080/1359432X.2017.1363185
- Weatherbee, T. G. (2006). A case of cyberdeviancy : Cyberaggression in the workplace Human Resource Management Review Counterproductive use of technology at work : Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, 20(1), 35–44. doi:10.1016/j.hrmr.2009.03.012

West, B., Foster, M., Levin, A., Edmison, J., & Robibero, D. (2014). Cyberbullying at Work : In Search of Effective Guidance. *Technology, Social Media and Laws*, 3(3), 598–617. doi:10.3390/laws3030598

ADDITIONAL READING

Borstorff, P., & Graham, G. (2006). E-Harassment: Employee Perceptions of E-Technology as a Source of Harassment. *The Journal of Applied Management and Entrepreneurship*, 11(3), 51–67.

Erdur-Baker, Ö. (2009). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools. *New Media & Society*, 12(1), 109–125. doi:10.1177/1461444809341260

Farley, S., Coyne, I., Axtell, C., & Sprigg, C. (2016). Design, development and validation of a workplace cyberbullying measure (WCM). *Work and Stress*, 30(4), 293–317. doi:10.1080/02678373.2016.1255998

Giumetti, G. W., McKibben, E. S., Hatfield, A. L., Schroeder, A. N., & Kowalski, R. M. (2012). Cyber Incivility @ work: The new age of interpersonal deviance. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 148–154. doi:10.1089/cyber.2011.0336 PMID:22304404

Heatherington, W., & Coyne, I. (2014). Understanding individual experiences of cyberbullying encountered through work. *International Journal of Organization Theory and Behavior*, 17(2), 163–192. doi:10.1108/IJOTB-17-02-2014-B002

Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, Behaviours and Definition in Three European Countries. *Australian Journal of Guidance & Counselling*, 20(2), 129–142. doi:10.1375/ajgc.20.2.129

Snyman, R., & Loh, J. M. (2015). Cyberbullying at work: The mediating role of optimism between cyberbullying and job outcomes. *Computers in Human Behavior*, 53, 161–168. doi:10.1016/j.chb.2015.06.050

KEY TERMS AND DEFINITIONS

Cyberbully: A person who directly or indirectly uses technology to reduce another person to a psychologically inferior state.

Cyberstalking: A form of harassment where the cyberbully makes continuous threats and sends inappropriate messages to an individual in the form of text messages, instant messaging, social media, emails.

Digital Evidence: Information that is stored and transmitted on digital devices.

Information and Communication Technology (ICT): Telecommunication technologies that provide access to information such as the internet, wireless networks, cell phones, and other communication mediums.

Masquerading: The creation of an anonymous or fake identity by an individual to harass another individual.

Traditional Bullying: An escalating process in which one or more employees are subjected to negative psychological and physical abuse recurring over an extended period of time, where the target is reduced to a psychologically inferior state and it creates a hostile work environment to those exposed.

Workplace Cyberbullying: An escalating process in which an employee is subjected to perceived psychological abuse recurring over a period of time where the perpetrator uses some form of technology.

Cyber Crime Against Women and Girls on Social Sites in Bangladesh

Fardaus Ara

 <https://orcid.org/0000-0002-0318-4576>

Rajshahi University, Bangladesh

INTRODUCTION

The advent of the Internet and modern communication devices with multiple features like camera, radio, general packet radio service and Wi-Fi networks and the wide diffusion of social media have made dramatic changes in human lives. It has created a virtual world with no boundaries; allows people to develop both personal and professional relationships across borders. The World Wide Web (WWW) permits users to disseminate content in the form of text, images, video, and audio. Worldwide, the number of people using the Internet is increasing day by day (Mala, 2016; UN Broadband Commission for Digital Development, 2015). As of June 30, 2018, more than half of the total world population i.e. 4.2 billion (55.12%) is using the Internet (Internet World Stats, 2018) for entertainment, business, education, information sharing and other purposes. In addition, social networking websites (SNWs) like Facebook, MySpace, YouTube, Flickr, LinkedIn, Snap chat, Twitter have developed a new platform to meet people. Around 2.62 billion people use different social network sites (Statista, 2018). It allows people to share ideas, pictures, posts, activities, events, and interests with people in their network. Regardless of any distinction, women in society are enjoying this liberation. It allows them to share their experiences with the whole world; their success stories as well as their problems (Halder & Jaishankar, 2009).

However, social sites have also created avenues for various criminal activities. Cybercriminals abuse the technology to abuse people for financial gain, to take revenge, to defame, to ridicule and humiliate for their self-enjoyment and so on. Therefore, social sites put people at risk while it makes life easier, safer, and more social. Pew Research Center (2014) reports that 73% of the adult Internet users have witnessed someone be harassed online and 40% have personally experienced it. The Internet Crime Complaint Center, known as IC3 received 3,463,620 cybercrime complaints since its inception. According to the IC3 report, the total cybercrimes reported in the US shows a steady increase from 2013 to 2015. In 2013, the number of cybercrimes reported was 262,813; in 2014 it was 269,422 and in 2015 it further augmented to 288,012. The Office for National Statistics reported that there were 5.1 million estimated cybercrimes and scams in England and Wales in 2014 (Mala, 2016).

Women are more vulnerable to cyber threats than men are as the offenders were unaccountable for the offences they commit. Moreover, the criminals are committing traditional crimes using the latest information technology as committing the crime is easier and investigating it gets tougher. In the contemporary world, instances of cybercrimes against women are increasing alarmingly (Halder & Jaishankar, 2009). According to the United Nations Broadband Commission Report (2015), women aged 18 to 24 years are at risk of cybercrime victimization. EU estimates show that one in ten women has experienced some form of cyber violence since the age of 15 and the impact on their lives is far more traumatic (European Institute for Gender Equality, 2017). Women are receiving unwanted emails often containing indecent and obnoxious language. The vulnerability and security of women is a major concern globally (Halder

DOI: 10.4018/978-1-5225-9715-5.ch048

& Jaishankar, 2008). According to IC3 (2015), in the US, 47.09% of the cybercrime complaints were reported by women. Women made 70% of the cybercrime complaints to the Working to Halt Abuse, a non-profitable organization, from 2000 to 2014 from all around the world. The organization further stated that 42% of the victims did not report their victimization (Mala, 2016). Statista (2017) reports that worldwide 57% of the surveyed women experienced abuse or harassment via Facebook.

Like other parts of the world, the number of Internet users is growing very fast in Bangladesh specifically, through mobile networks. There are 85.92 million Internet subscribers as of April 2018 and among them, 29 million are registered Facebook users; one-third of the subscribers of the Internet are women (BTRC, as cited in Akter, 2018). The average time people stay on Facebook and other social sites has gone up in recent times. People consciously or unconsciously reveal too much of their personal life. Bangladesh ICT Division's Cyber-Help Desk received more than 17,000 complaints; women made 70%. It is found that more than 60% of women faced some form of harassment on Facebook; about 10% of them filed complaints that their images were stolen, merged with pornographic images, and made available on the Internet (Rabbi, 2017). However, they mostly avoid legal assistance due to social stigma.

The Cyber Crime Awareness Foundation Bangladesh (CCABD) reports that 51.13% of women are victims of cybercrime. Women belonging to age group 18 to 30 years mostly become the victim of such crimes (73.71%), while 0.52% are below the age of 18, and 12.77% are of 30 to 45 years and 3% are above 45 years of age. Women Facebook users are often victims of fake accounts and hacking. Once a fake account is created, the stalker spreads propaganda through the accounts; study reveals that 9.77% of women are the victims of such stalking. In addition, the offender can easily send threatening messages to the victim and harass her ("51.13pc women harassed on social media," 2018). However, identifying criminal is a difficult job due to the lack of evidence and fear of defamation.

OBJECTIVES

The objectives of this study are:

- To understand the impacts of cybercrime on women in Bangladesh;
- To find out existing schemes and mechanisms to deal with the offenders of cybercrime; and
- To explore remedial measures to protect women and girls against cybercrime.

LITERATURE REVIEW

Research on cybercrime against women and its consequences is an emerging field. There have been a number of studies on cybercrime against women in the international arena.

Sankhwar and Chaturvedi (2018) recognized cybercrime as a major challenge facing law enforcement agencies in India. They claimed that digital space in India opened doors to cybercriminals and the offenders used the cyber platforms to harass and abuse women and children. They focused on the existing legislative intervention measures and prescribed a few suggestions to curtail cyber-crime against woman and children.

Uma (2017) explored common forms of cybercrimes committed against women in India. She claimed that the existing provisions regarding information technology failed to realize women's experiences. The study recommended amendments in the laws to ensure remedies for the female victims of cybercrime.

Singh (2015) discussed the reasons for and forms of cybercrime against women in India. The study further focused on the impact of cyber violence on their social life and gave some suggestions to curb cybercrime against women.

Winkelman, Early, Walker, Chu, and Yick-Flanagan. (2015) examined women's experiences with and attitudes toward cyber harassment on social media in the USA. The study found around 20% of the participants received a sexually obscene message on the Internet. Moreover, more than 10% of repetitively received pornographic messages from strangers. Among the victims, more than a third reported feeling anxious and one-fifth noticed changes in their sleeping and eating patterns as well as feeling helpless due to the harassment.

Gitonga (2014) studied the effect of Internet crimes on women students at the University of Nairobi. The researcher claimed that female victims of cyber oppression and attacks may fail to utilize the benefits of the Internet. Conversely, they might stop using the Internet to protect themselves. Therefore, the Internet worked as a double-edged sword because it empowers and put users at risks.

Sissing (2013) in a study on cyberstalking in South Africa found that women belonging to the age group of 18 to 25 years were the main victim of cybercrime. They further claimed that the female victims were cyberstalked through social networking sites by outsiders.

Halder and Jaishankar (2011) conducted a comparative study to examine the criminal justice systems regarding protection of women harassed online in countries like the United States, the UK, and India. They claimed that the judicial interpretations of the term "gender harassment" have caused secondary victimization of women as many of the cybercrime activities have not been legally interpreted as "gender harassment" in the laws. As a result, the police are often not interested to investigate properly, and the trial may fail to help the victim due to a lack of relevant laws that make the female victims suffer.

However, scholarships on cybercrime against women in Bangladesh are scanty. For instance, Kabir (2018) discussed the extent and types of online/cyber violence and harassment against women and girls and its impact on their daily lives. She further shed lights on the existing laws and regulations to combat cybercrime in Bangladesh.

Ahmed, Kabir, Sneha, and Jafrin (2017) focused on female Facebook users in Bangladesh. They also identified the threats and risks associated with the disclosure of their personal information on Facebook. This paper also suggested some remedial measures to facilitate their rights to online privacy.

Cybercrime against women is at an alarming state in Bangladesh; it has caused the most traumatic experience for women. There is a need to inform about the pervasiveness and different forms of cybercrimes taking place against women and girls and to make them aware about the safety precaution when utilizing the Internet as well as the existing remedial measures. This study is expected to fill the research gap, as a few scholarships on cybercrime against women using social sites in Bangladesh are available.

METHODOLOGY

This study followed a qualitative case study method to understand the nature and types of cybercrime committed via Facebook and Messenger against women as well as the effect of cybercrime on their lives. The participants were approached by sending private messages on Facebook Messenger and 35 agreed to participate. However, participants were selected only if she was a victim of cybercrime on Facebook and/or Messenger. Finally, 12 were selected for semi-structured online interviews. The interview questions were designed to collect background information like age, education, and occupation of the participants as well as to collect information on their experience of harassment on Facebook and Messenger and their

opinions on how their rights can be protected on social sites. Participants were asked whether they used safety tips like locking personal albums, information, and personal walls of social networking sites, or shared emotions/feelings with virtual friends whom they did not meet in real life. In addition, Secondary data were collected from books, journals, reports, newspapers, documents, and the Internet.

Responses to questions obtained from each participant were coded in the same category. Then data was coded into analytical units. Raw data were organized in order to develop findings, conclusions and recommendations manually. Results were presented through narrative text, simple computations, and analytical reasoning.

CYBERCRIME

Cybercrime is a universal problem now. The first cybercrimes took place in India, Japan and China in 1820. Gradually, extent, type and nature of cybercrime increased and by mid of 20th century, it became a serious issue globally. Around the world and in the Middle East and third world countries the expansion of Internet connectivity in recent years has led to the increase in cybercriminal activities (El-Guindy, as cited in Kamal, Chowdhury, Haque, Chowdhury, & Islam, 2012). There is no specific or universal definition of cybercrime as different agencies and researchers define the concept based on their context. It is also known as “computer crime,” “computer-related crime,” “high-tech crime,” or “Internet crime” (Brenner & Goodman, as cited in Kamal et al., 2012). A new dimension of cybercrime is adding almost every day.

Wall (2005; 2008/11) asserts that cybercrime refers to insecurity in cyberspace. The term generally refers to any harmful activity that is in some way related to the misuse of computers, more recently suggesting to networked computers. The Council of Europe (2001) suggests the following acts as cybercrime:

- Offences against the privacy, integrity and obtainability of computer data and systems;
- Traditional computer-related crimes;
- Content related offences;
- Breach of copyright and crimes to related rights; and
- Crimes involving the violation of privacy.

The Lawyers and Jurists Bangladesh (2017) defines cybercrime as a criminal activity that may range from illegitimate access through the computer; transmissions of computer data to, from or within a computer system illegally; unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; misuse of devices; forgery/theft, and electronic fraud. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts or inventing and spreading viruses on other computers or publishing secret information on the Internet. Therefore, cybercrime is an offence committed with a criminal motive using modern telecommunication networks like the Internet. Cybercrimes can take place against an individual, against the organization, against the economy, against society or against the state (Hanif, 2016).

COMMON FORMS OF CYBERCRIME AGAINST WOMEN ON SOCIAL SITES

Women especially young girls with little or no experience about the cyber world are an easy victim of cyber criminals who may be either male or female. The extent of victimization depends on a number

of factors, like, the sexuality of the victim, her ideologies, marital status, profession, the regularity of her partaking in selected groups, the language she uses, her popularity in the groups and so on. Male offenders mostly attack the victim for sexual purposes like morphing, using the image for pornographic purposes, cyberstalking etc. and non-sexual purposes such as harassment and bullying. However, female criminals attack the victim mostly due to ideological differences, hatred or taking revenge (Halder & Karuppannan, 2009). The offences against women and girls occur in the social sites are:

Cyber Verbal Abuse by Groups of Perpetrators Spreading Hate: A female member of the social site may be attacked by a group of criminals both in the community wall and also in her own message board (Halder & Jaishankar, 2008).

Cyber Defamation Targeting the Individual: The male member spread lies about the female member to other members through his own posts, community walls etc. after emotional breakups (Citron, 2009; Halder & Jaishankar, 2008).

Cyberstalking: Women and children are the most likely targets of cyberstalking. Here the offender uses the Internet to stalk someone for online harassment and abuse. A cyberstalker follows the victim's online activity, collects information, and makes threats and intimidates verbally (Halder & Karuppannan, 2009; Sankhwar & Chaturvedi, 2018).

Morphing: The criminals download an original picture of the victim from social media, or some other sources, edit and upload morphed photos on social media sites or porn sites for pornographic purposes (ibid).

Cloning: Cloned or fake profiles of female victims are created using her personal information. The cloned profile makes people confused. The cloned profile sends add requests to the victim's friends and crack their privacy for evil purposes. This is very common in social sites like Facebook, Myspace and Orkut (Halder, 2007).

Cyber Obscenity: The victim's photograph is used, morphed and distributed on the Internet with indecent postures. The attacker may also post obscene messages on her wall (Citron, 2009).

Hacking: Personal information of the victim is used for evil purposes. Targets are chosen and their profiles are hacked for sexual purposes. The harasser may even distribute open invitations for having sex with the profile owner at her home address (Citron, 2009; Halder, 2007; Halder & Jaishankar, 2008).

Cyberharassment: It may take the form of continuous messaging to the profile's wall or personal e-mail address, regular spying and messaging in her wall, constantly sending friend requests, become a member of groups where she is a member etc. (Citron, 2009; Halder, 2007).

Virtual Rape: Virtual rape is a violent type of cyber victimization where the targeted woman is taken up by a harasser with messages like "I will rape you," or particular group members may attack together with slang and dirty words that lead other members to comment on the victim's sexuality. The profile owner becomes a hot topic for erotic conversations or addressing by vulgar name etc. (Citron, 2009).

Cyberbullying: The offender may continually bully the target in the social sites where either he or she is a member. Women are the most likely targets for their sexuality, emotional breakup or even domestic violence by their ex-spouse or ex-lover (Citron, 2009; Halder & Jaishankar, 2008).

Impersonation and Cheating: Social sites allow for creating multiple ids under pseudo names, hiding one's real age, sex and other information. This gives the culprits the opportunity to flirt with women members (Halder & Jaishankar, 2008). The harasser convinces the victim in such a way that she is encouraged to share her secrets, and even have erotic chats with the criminal. When the victim puts pressure to meet the offender physically, he blackmails the victim or cheats the victim (Halder & Jaishankar, 2009).

IMPACTS OF CYBER CRIME ON WOMEN IN BANGLADESH

West (2014) conducted research on cyber violence against women in the US. She found several psychological, social, physical, and economic impacts of cyber violence on women. The most dominant emotional impact on women ranges from anxiety to thoughts of suicide and engaging in self-harming behavior. Cybercrime, particularly nonconsensual distribution of images and revenge porn against women might have serious and detrimental economic effects on women. Women might lose their jobs because of their nude picture circulated on the Internet. Revenge porn images and defamation may create lifetime troubles for women and make it difficult to get new jobs or progressing in their present job. Cybercrime can exacerbate or lead to physical violence against women. If the offender is refused, he may attack the victim physically. The social impacts for women can be very severe. They might feel isolated from friends and family. Her friends and family may turn against her. Therefore, often women act in accordance with their abuser's threats to avoid such repercussions. Furthermore, the victim withdraws herself from online activities.

The situation is similar in Bangladesh. Women and young girls who use digital platforms experience some form of cybercrime over their lifetime. However, morphing, cyberstalking and cyber pornography including revenge porn are the most common cybercrimes committed against women to destroy their personal reputation, create fear and monetary losses. Bangladesh is a country where gender-based harassment committed in public spaces, homes and workplaces go unpunished. Therefore, victims of cyber sexual harassment and/or cyberbullying barely report in public or complaint to the police (Preetha, 2015; Supan, 2015).

Bangladesh is a conservative society where the effects of cybercrime not only affect women victims; it has a chain reaction on their families. Majority people have a tendency to believe everything posted on social media due to lack of awareness, ignorance, and education. They enjoy such content and like to spread gossip that intensifies the victim's suffering by a thousand times. The victim's family members also face social exclusion, humiliation and public resentment (Karaman, as cited in Akter, 2018). Such criminal act may lead to depression, guilt, humiliation, and fear of harm to self and family members and destroy the victim's career, education, and social life. Some victims take the route of drug addiction while some commit suicide. Only a few of the victims recover from such a tragedy. From 2010 to 2014, Bangladesh National Woman Lawyers' Association identified 65 suicide attempts by female victims due to cybercrime. In addition, every year, on average, 11 suicide attempts by women take place because of cyber violence (BNWLA, as cited in Akter, 2018). A few examples of cybercrimes committed against the participants:

Case 1

Ms X is a third-year university student using Facebook for the last five years. She had no idea of cyber-crime on social sites and accepted friend requests from all. She made a special Facebook friend who claimed himself a final year medical student in another city. Their online relation was so close. One day the boy asked for some explicit pictures of her. She gave him the photos. Afterwards, they met in person twice. Subsequently, he demanded to have physical sex that she refused. The man then began to send her nude images and adult videos with derogatory comments about her appearance and character. She blocked him. He then blackmailed her and threatened to inform her parents and relatives. She felt helpless and afraid of sharing this incident with her family. Because of fear, she was compelled to fulfil his

demand. She does not want to make any complaint formally due to afraid of spreading the news among her family members and still under the grip of that man.

Case 2

Ms Y is a Master degree student at a University. She met a boy on Facebook which turned into a love affair. She spent some private moments with him at a hotel room for three to four times. Suddenly, the boy started blackmailing her for money threatening to spread private moment's videos of her on the Internet which was captured with a hidden camera. She informed her family members. Fortunately, her family was very supportive and they filed a case to the police.

Case 3

A year 12 student was a member of Facebook. Her cousin who once proposed her and was refused by her used Facebook to humiliate her. He spread messages on Facebook that the victim was responsible for shattering his life. Relatives and friends of the perpetrator trusted the gossip and started molesting and abusing the victim. She was sleepless for several nights; had an eating disorder; felt helpless and isolated as her friends and family members started avoiding her. She lost her concentration on studies. She was so frustrated that tried to commit suicide. At last, her family took her to a psychiatrist for treatment.

Case 4

A working woman suffered as her Facebook accounts were hacked several times. The offender was ex-husband of her. They both were members of a similar Facebook group. The perpetrator started following her after their divorce. He stalked the victim regularly and contacted her friends to harass her. She was so upset that failed to concentrate on her job for several weeks. She could not communicate with her colleagues at the office. The incident affected her professional career. Hre ex-husband took help from a hacker to hack her account. The hacker hacked her account, posted unpleasant pictures on her wall, and tried to blackmail her. The woman felt panicked and made a complaint to the police.

The magnitude of such incidents is increasing day by day in Bangladesh. Ahmed et al. (2015) conducted a study on cybercrimes against women. The study found 36.8% users had been harassed, and 78.9% faced unusual situations, which can be treated as harassment. 84.2% of users had been harassed by the people with whom they are connected at Facebook. Most of the harassment around 27% is coming from the unknown people met at the Facebook first time. The study also found 10.5% harassment from completely unknown and 5.3% from a known person. The interview data revealed that as the female users are less concerned about the privacy settings of Facebook, their profile and personal information or photos were accessible by every registered Facebook users and they remained the easy target of the cybercriminals.

It is a common practice among young girls of making friendship with a stranger on Facebook and share personal feelings with him. At first, the girl fails to realize the consequence of entering into a relationship with a stranger. The problem arises when the so-called Facebook friend starts to exploit her emotions and feelings. In most of the time, the victim feel helpless and frustrated, has no idea about what to do or where to seek help. As the victim feels that reporting the incidents would lead her to face intrusive questions about her character and bring disgrace to her and her family rather than justice, she does not seek legal remedies (Kabir, 2018; Preethi, 2015). Similar findings were revealed during interview ses-

sions with the participants. Most of them did not want to complain or inform their family due to fear of humiliation. Moreover, women who try to report or file cases have to experience further victimization and harassment. Deep-rooted patriarchal attitudes of the institutions rather make the situation worse for women. For example, if a woman visits the police with complaints that her explicit pictures are being spread on the net, the police (may) seem more interested to listen about her relationship in detail and staring at the pictures than helping her. In this situation, even if a woman is courageous enough to report the crime, it does not guarantee justice finally. Furthermore, law enforcement agencies often do not have the technical expertise or intention to address cases of cyber sexual harassment as it is often difficult to track or identify the perpetrators because of fake profiles and addresses (Preethi, 2015).

LEGAL PROCEDURES AND MEASURES TO COMBAT CYBERCRIME IN BANGLADESH

There is a lack of universally recognized law, convention, or rules to deal with cybercrime taking place in the social sites. Moreover, the majority of the social site users are registered under the US laws section 230 of the Communication Decency Act, 1996 that protects them from being charged as an offensive media. However, this creates a problem for victims, especially women. In addition, the meaning of obscenity varies across societies. The US has the Violence Against Women and Department of Justice Reauthorization Act of 2005 to protect women from cyber-harassment or cyberstalking. In contrast, the UK does not have any specific law to protect cyber offences against women. However, there are several laws like the Computer Misuse Act 1990, Police and Justice Act 2006, Sexual Offences Act 2003, The Prevention of Sexual Offences (Scotland) Act 2005, Protection from Harassment Act 1997, Malicious Communications Act 1988 to prevent cybercrime against women. Nevertheless, cyber offences are not legally defined that allows criminals to escape punishment very often. Canada controls the online victimization of women through specific chapters of Canadian Criminal code applicable for both gender and there are no special laws to protect women. Indian law does not recognize many of the offences that occur online like cyberbullying, cyber eve teasing, cyber-harassment, cloning of the profile etc (Halder & Jaishankar, 2009; 2011).

The Government of Bangladesh (GOB) has adopted several initiatives and laws to control and prevent cybercrime. The Constitution of Bangladesh ensures equality before the law to all its citizens irrespective of sex and prohibits all types of discrimination. However, there is no comprehensive law or section adequately dealing with sexual harassment in social media and other digital platforms.

Section 500, 504 and 509 of the Bangladesh Penal Code, 1860 imposes a penalty for defaming any person. However, the Penal Code is more than 150 years old and not effective to deal with online harassment today. The Nari O Shishu Nirjatan Daman Ain (Suppression of Violence against Women and Child Act), 2000 penalizes 'sexual oppression' including any indecent gesture and the disclosure of the identity of a victim in the media as an offence.

According to section 69 of the Bangladesh Telecommunication Control Act, 2001 sending any obscene or indecent message is a punishable offence. Nevertheless, the 'Telecommunication Act 2001' does not address the gender-based violence that takes place on the Internet (Kabir, 2018).

Section 57 of the Information Communication Technology Act 2006 (amended 2013) has provision for penalty of maximum 10 million BDT as fine and a maximum jail sentence of 14 years and minimum seven years imprisonment if someone (male/female) publishes fake, obscene or defamatory information in electronic form that causes to deteriorate law and order, prejudice the image of the State or person or

causes to hurt religious belief. It also states that the crime is non-bailable. However, the Act does not define gender-based violence online or not define what constitutes “obscene” that helps the criminals to escape punishment (Ahmed et al., 2017; Akter, 2018; Kabir, 2018).

The Pornography Control Act, 2012 states that if any person produces or agrees to supply participants to make pornography, or forces any person to take part in the production of pornography, he/she will be punished for a maximum of five years imprisonment and a fine of 2,00,000 BDT. Moreover, the production of pornography is also punishable by a maximum of seven years sentence and a fine of 2,00,000 BDT. Furthermore, this is a non-bailable offence. However, the Pornography Control Act fails to properly control and combat the heinous crime due to institutional corruption and powerful allies of the criminals with the ruling party. The offender remains safe if he has power and the victims are poor (Akter, 2018; Kabir, 2018).

The GOB has established a fast-track court (2013) to deal with cybercriminals and complete trials within six months. In addition, GOB has formed a ‘Cybercrime Tribunal’ to address cyber violence. However, 90% of victims do not complain to the Tribunal. The Right to Information (RTI) Act states that from 28 July 2013 to 10 February 2016, the Cybercrime Tribunal received 520 cases of which 328 cases were dropped (Ahmed et al., 2017; Akter, 2018). Furthermore, Bangladesh police have opened a cyber-wing to deal with cyber threats. The wing also monitors cybercrimes and tracks the criminals. Additionally, Bangladesh Telecommunication Regulatory Commission (BTRC) is working to regulate and monitor cybercrime. This commission blocks inappropriate websites, blogs, and Facebook accounts if necessary (Akter, 2018).

The draft Digital Security Bill, 2016 later amended in 2018 has been presented in the parliament (Parliament Correspondent, 2018). It is expected that the act will assist to combat cybercrime in Bangladesh. This act empowers the GOB to establish National Digital Security Agency (NDSA) headed by a Director-General to monitor, observe and take necessary steps in respect of all the Bangladeshi computers or digital systems, networks, mobiles or digital communication (voice and data) networks to secure, prevent and curb cybercriminal activities in Bangladesh. In addition, NDSA is allowed to establish a digital forensic lab for cyber forensic analysis and Bangladesh Cyber Emergency Response Team (Bangladesh-CERT) for an instant response against cybercrimes. Besides, The Act has the provision of establishing a National Digital Security Council (NDSC) chaired by the Prime Minister to discuss cyber-related issues and take immediate decisions. All the offences committed under this act are triable in the cyber tribunal and cyber appellate tribunal established under the ICT Act, 2006 (Hanif, 2016).

RECOMMENDATIONS

In Bangladesh, the lawmakers and enforcers are interested to satisfy the ruling elites. Therefore, it is seen that the digital act is more concerned about the denigration of the prime minister and the president rather than protecting the women. Bangladesh government has adopted several cyber laws but the laws are not implemented properly. It is mostly seen that the victims feel hesitated to ask for legal assistance due to various reasons, especially for social humiliation. As these cyber laws have many loopholes, the offenders repeat the crimes repeatedly. In addition, the criminals get themselves free by giving bribes to the law agencies or through threats. Therefore, the existing acts need to be revised incorporating provisions for offences like cyber harassment; cyberstalking; violation of privacy; online trafficking and so on. Furthermore, there is a need to ensure strict penalties for cyber offences in order to discourage such offences in the future.

The GOB needs to revise the applicable regulatory framework through consultation along with the Bangladesh Telecommunication Regulatory Commission, which is more powerful to control any website, explicit contents or online based websites. Moreover, GOB may develop a broad framework with mobile service providers and Internet providers. Furthermore, Internet Service Providers and mobile companies providing or hosting social media services must be made accountable. They have to report criminal activities committed through their services; take away any criminal or offensive content, disclose the identities of such perpetrators. The identity of the complainants in both civil and criminal proceedings brought by women must be maintained strictly.

Digital Literacy and awareness campaign at the root level is must to prevent cybercrime against women and girls. Seminars and symposiums on cybercrimes, online privacy, possibilities and limits of the Internet and social sites, how to deal with such incidents, legal remedies need to be arranged regularly with women activists, teachers, responsible authorities, parents and young girls and boys. Open discussion between the government and the academics, civil society, youth-led organizations, legal aid based organizations, cybercrime specialists, and law enforcement agency is a must to deal with the problem.

The complex nature of cybercrime makes the investigation difficult for the law enforcing agencies as they are not well trained and equipped. The Police force and investigating agencies must be trained to tackle and handle cybercrimes. A guideline on how to use cybercrime related law may be developed. A Digital Police Portal or E-Portal may be established where victims can report their problems online.

Women groups and civil society should advocate for relevant legal and policy reform. In addition, they need to strengthen their existing networks and collaboration with government institutions. They may introduce awareness-raising program and training on cybersecurity.

School curriculum must be designed in such a way so that it covers all aspects of cybercrimes. Girls should be educated especially all types of cybercrimes and how to handle them. Media campaign on awareness building regarding uses of the Internet and security is essential. The attitude of the society towards women needs to change so that the victim woman do not feel isolated or helpless. Internet users need to be educated on privacy policy and their rights online.

The lack of universal laws to regulate social networking websites and the lack of legal recognition of the offences committed against women online has instigated the growth of cyber victimization of women (Halder & Jaishankar, 2009). Therefore, developing global cooperation is essential to deal with cases, as cybercrimes have no boundaries.

CONCLUSION

The growth of cybercrime on social sites in Bangladesh is on the rise. People use social sites for communication, information sharing, education, business and other purposes. However, it brings privacy threats due to some dishonest people. The problem is not using the technology rather using it unconsciously that affects women users largely. Due to the conservative culture, women still are not ready to report cybercrime immediately. Patriarchal norms and values are practised by men to establish control over women by committing crimes on social sites. As there are loopholes in the laws, the criminals commit the crimes frequently. The law enforcing agencies must deal with the cases on an emergency basis to create an example. There is a need for constant evaluation of cyber laws and procedure because women face difficulties while seeking justice due to lack of awareness. The GOB, civil society groups, NGOs, and women organizations need to work in collaboration to curb and control cybercrime.

FUTURE RESEARCH

The study only focuses on social sites specifically on Facebook and Messenger. Further study may be conducted on the ICT Act of Bangladesh and its' impact on women. In addition, a comparative discussion on the effect of cybercrime on urban and rural societies in Bangladesh may be an interesting research topic. Moreover, research may be designed to explore the status and nature of female cybercriminals in Bangladesh. Further research can be designed for investigating other social networking sites.

ANNEXE

The researcher arranged semi-structured interviews on Facebook Messenger with 12 female Facebook users. While they were asked, “are you a victim of cybercrime?” All of the participants admitted to being victims of cybercrime via Facebook. In majority cases, the offenders were an online friend whom they did not know before.

The question was asked, “do you know about Facebook privacy rules?” Nine of them said of being aware of the privacy settings. However, they did not maintain privacy and kept their profiles ‘public.’

Participants were asked to share their mental, social, and physical state after being harassed or abused online. They felt isolated and afraid of spreading the news among their family and friends. Therefore, they initially did not disclose the incidents. Later on, a few of them shared it with their close friends or family members and only two of them sought legal help.

While asking “do you know where and how to complain”? Surprisingly, 11 said of not being fully aware of the complaining procedure. However, seven of the victims said that they heard about it when one of their friend or family members informs them.

Participants were asked whether they know about the legal measures and laws relating to cybercrime in Bangladesh. Unfortunately, all were unaware of any cybercrime related laws. The GOB has launched 24 hours of national helpline for women and children. The hot number is 109. In addition, there is another police Emergency service 999. None of the participants was familiar with the services.

Regarding the punishment of the criminals, all of them said for an exemplary one like life- imprisonment so that the offender would never repeat the heinous act again. In addition, they said for attitude changes in the society towards women and new laws to combat digital crime.

REFERENCES

51. 1.3pc women harassed on social media. (2018, May 27). *Bangla Insider*. Retrieved from <https://en.banglainsider.com/ict/2482/51.13pc-women-harassed-on-social-media>
- Ahmed, S., Kabir, A., Sneha, S. S. A., & Jafrin, S. (2017). Cyber-crimes against womenfolk on social networks: Bangladesh context. *International Journal of Computers and Applications*, 174(4), 9–15. doi:10.5120/ijca2017915407
- Akter, F. (2018, June 17). *Cyber violence against women: The case of Bangladesh*. Retrieved from <https://www.genderit.org/articles/cyber-violence-against-women-case-bangladesh>
- Bartlett-Bragg, A. (2006). *Reflections on pedagogy: Reframing practice to foster informal learning with social software*. Retrieved from: <http://www.dream.sdu.dk/uploads/files/Anne%20Bartlett-Bragg.pdf>

Burke Winkelman, S., Oomen-Early, J., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring cyber harassment among women who use social media. *Universal Journal of Public Health*, 3(5), 194–201. doi:10.13189/ujph.2015.030504

Citron, D. K. (2009). Cyber civil rights. *BUL Rev.*, 89, 61–125.

Council of Europe. (2001). *Convention on Cybercrime*. Retrieved from coe.int/Treaty/en/Treaties/Html/185.htm

European Institute for Gender Equality. (2017). *Cyber violence is a growing threat, especially for women and girls*. Retrieved from <https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls>

Gitonga, W. (2014). *The prevalence of internet crimes on women students at the University of Nairobi (Masters thesis)*. University of Nairobi. Retrieved from http://erepository.uonbi.ac.ke/bitstream/handle/11295/75135/Wanjiku_The%20prevalence%20of%20internet%20crimes%20on%20women%20students%20at%20the%20University%20of%20Nairobi.pdf?sequence=3&isAllowed=y

Halder, D. (2007, June). Cybercrime against women in India. *CyberLawTimes.com*. Retrieved from <http://www.cyberlawtimes.com/articles/103.html>

Halder, D., & Jaishankar, K. (2008). Cyber crimes against women in India: Problems, perspectives and solutions. *TMC Academic Journal*, 3(1), 48–62.

Halder, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. *The Journal on Victimization*, 12(3), 5–26. Retrieved from <https://ssrn.com/abstract=1561774>

Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders*, 6(4), 386–398. doi:10.1080/15564886.2011.607402

Halder, D., & Karuppannan, J. (2009). Cyber socializing and victimization of women. *Temida*, 12(3), 5–26. doi:10.2298/TEM0903005H

Hanif, M. A. (2016). Exploration of cybercrime and cyber law: Growth of the state concerns and initiatives with special focus to the context of Bangladesh. *Prime University Journal of Multidisciplinary Quest*, 10(1), 1-22. Retrieved from http://www.primeuniversity.edu.bd/070513/journals/v_10_n_1_J_J_2016/Exploration.pdf

Internet World Stats. (2018). *Internet usage statistics: The internet big picture world internet users and 2018 population stats*. Retrieved from <https://www.internetworldstats.com/stats.htm>

Jeet, S. (2012). Cyber crimes against women in India: Information technology act, 2000. *Elixir International Journal Elixir Criminal Law*, 47, 8891–8895.

Kabir, N. (2018). *Cybercrime a new form of violence against women: From the case study of Bangladesh*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3153467

- Kamal, M. M., Chowdhury, I. A., Haque, N., Chowdhury, M. I., & Islam, M. N. (2012). Nature of cybercrime and its impacts on young people: A case from Bangladesh. *Asian Social Science*, 8(15), 171–183. doi:10.5539/ass.v8n15p171
- Mala, G. (2016). *Cybercrime victimization: a study among women victims in Chennai city (PhD thesis)*. Chennai, India: University of Madras. Retrieved from <http://hdl.handle.net/10603/179462>
- Parliament Correspondent. (2018, April 10). Digital security bill 2018 presented in parliament. *bdnews24.com*. Retrieved from <https://bdnews24.com/bangladesh/2018/04/10/digital-security-bill-2018-presented-in-parliament>
- Pew Research Center. (2014). *Online harassment*. Retrieved from <http://www.pewinternet.org/2014/10/22/online-harassment/>
- Preetha, S. S. (2015, May 16). Digital sexual harassment in digital Bangladesh. *The Daily Star*. Retrieved from <https://www.thedailystar.net/in-focus/digital-sexual-harassment-digital-bangladesh-82480>
- Rabbi, A. R. (2017, September 21). Women biggest victims of rising cyber crimes. *Dhaka Tribune*. Retrieved from <https://www.dhakatribune.com/bangladesh/crime/2017/09/21/women-biggest-victims-rising-cyber-crimes>
- Sankhwar, S., & Chaturvedi, A. (2018). Woman harassment in digital space in India. *International Journal of Pure and Applied Mathematics*, 118(20), 595–607.
- Singh, J. (2015). Violence against women in cyberworld: A special reference to India. *International Journal of Advanced Research in Management and Social Sciences*, 4(1), 60–76.
- Sissing, S. K. (2013). *A criminological exploration of cyberstalking in South Africa (Masters thesis)*. University of South Africa. Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/13067/dissertation_sissing_sk.pdf?sequence=1
- Statista. (2017). *Share of women worldwide who have ever experienced abuse or harassment on selected websites and social media platforms as of July 2017*. Retrieved from <https://www.statista.com/statistics/784821/harassment-women-websites-social-media-platforms/>
- Statista. (2018). *Number of social network users worldwide from 2010 to 2021 (in billions)*. Retrieved from <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>
- Supan, Q. M. H. (2015, March 10). Cyber crimes. *The Daily Star*. Retrieved from <https://www.thedailystar.net/law-our-rights/cyber-crimes-70592>
- The Lawyers and Jurists. (2017). *Cyber crimes in Bangladesh*. Retrieved from <http://www.lawyersnjurists.com/article/cyber-crimes-bangladesh/>
- Uma, M. S. (2017, April). Outlawing cybercrimes against women in India. *Bharati Law Review*, 103–116.
- UN Broadband Commission. (2015). *Cyber violence against women and girls: A worldwide wake-up call*. Geneva: ITU & UNESCO. Retrieved from <https://en.unesco.org/sites/default/files/genderreport-2015final.pdf>

Wall, D. S. (2005). The internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 77-98). Thousand Oaks, CA: Sage Publications. doi:10.4135/9781452225708.n4

Wall, D. S. (2008/11). Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime (revised Feb. 2011). *Information Communication and Society*, 11(6), 861–884. doi:10.1080/13691180802007788

WestJ. (2014). *Cybercrime against women*. Retrieved from <http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf>

Winkelman, S. B., Early, J. O., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring Cyber harassment among women who use social media. *Universal Journal of Public Health*, 3(5), 194-201.

ADDITIONAL READING

Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: trends and challenges. In *Handbook of Asian criminology* (pp. 49-63). Springer. doi:10.1007/978-1-4614-5218-8_4

Gercke, M. (2012). *Understanding cybercrimes: Phenomena, challenges and legal response*. International Telecommunication Union. Retrieved from <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>

Haque, S. M. S. (2018). Freedom of thought and social networking in Bangladesh: Case analysis on Facebook. *Development and Change*, 3(1), 93–109.

Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (2014). A study on the cyber-crime and cybercriminals: A global problem. *International Journal of Web Technology*, 3, 172–179.

Salim, R. (2005). *Cybersecurity Bangladesh perspectives*. Paper presented at the ITU WSIS Thematic Meeting on Cyber Security, ITU Headquarters, Geneva, Switzerland.

KEY TERMS AND DEFINITIONS

3

Crime: Any illegal action that is considered an offence and is punishable by law.

Cyber: It refers to the features or characteristics of the culture of computers, information technology, and computer-generated reality.

Cybercrime: A crime that involves a computer and a network.

Internet: The Internet is an interactive medium based on a decentralized network of computers. The Internet may also be used to engage in other activities such as sending and receiving emails, money, trading files, exchanging instant messages, chatting online, streaming audio and video, every type of business purpose, and making voice calls.

Internet Crime Complaint Center (IC3): It was established to provide people with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation (FBI) regarding cybercriminal activities and to develop cooperation with law enforcement agencies.

Social Networking Site: A social site is an online platform where people build social networks or relations with other people who usually share similar interests. A social networking service is a platform that increases group interaction and shared spaces for collaboration, social relations, and aggregates information exchanges in a web-based environment (Barlett-Brag, 2006).

Wi-Fi: A popular networking technology that uses radio waves to provide wireless high-speed Internet and network connection.

World Wide Web: The world wide web (WWW) is a network of online content on the Internet that allows documents to be connected to other documents by a link and enable the user to search for information by browsing on the net.

Section 4

Financial Fraud, Identity Theft, and Social Manipulation Through Social Media

Internet Privacy

4

Nathan John Rodriguez

Weber State University, USA

INTRODUCTION

Technological innovations have fundamentally altered communication patterns during the past three decades. Smartphones have become widely adopted in recent years, and offer the allure of convenient access to news content, entertainment, retailers, weather information, and other people. In a practical sense, users sacrifice information regarding their online activity in exchange for content that is deemed relevant to their interests. There have been slightly different iterations of the axiom, “If the service is free, you are the product” over the past few decades, as it has come to signify the dangers of popular online platforms collecting consumer data (Oremus, 2018).

This entry examines internet privacy through four complementary, overlapping perspectives. It is argued that the most significant threats to internet privacy come through user activity, corporate data collection, governmental surveillance, and malevolent actors. To be sure, these are not discrete categories, but are frequently interrelated. For example, consumers frequently submit private information to corporate entities in exchange for access to online content. Before delving into further explanations and examples of these perspectives, it is necessary to begin with a discussion of what is meant by the notion of privacy and internet privacy.

BACKGROUND

Privacy Theories

One of the earliest definitions of privacy is “the right to be let alone” (Warren & Brandeis, 1890). The notion of privacy encompasses territorial privacy, personal privacy and informational privacy (Rosenberg, 1992). There are a variety of potential dimensions to informational privacy, but a broader definition of these concerns has been characterized as the unauthorized use of personal information. (Smith, Milberg, & Burke, 1996).

Online privacy studies have focused on the motivation for privacy protection as well as the behavior related to privacy protection. Internet privacy research frequently relies upon protection motivation theory (PMT), which posits that individuals engage in a rational thought process, and protect themselves based on the perceived severity of a negative outcome, the probability of that event occurring, and the efficacy of a potential solution (Rogers, 1975). PMT has undergone several iterations in recent years, and an extended parallel process model (EPPM) emerged to address these deficiencies by explaining why—even in the face of a high-perceived threat—a user may not change their behavior. Recent studies have shown that internet users “tend to ignore privacy risks until they encounter monetary loss online in person” (Chen, Beaudoin, & Hong, 2017, p. 300).

DOI: 10.4018/978-1-5225-9715-5.ch049

The Privacy Paradox describes the incongruent way in which users frequently express a theoretical interest in protecting their privacy, yet do not engage in behaviors that would protect their privacy (Norberg, Horne, & Horne, 2007; Brown, 2001). A thorough review of Privacy Paradox literature concluded that decision-making regarding privacy may be a rational calculation of risk and reward, a biased and irrational risk assessment, or a situation that involves virtually no calculation (Barth & de Jong, 2017). The authors concluded that decision-making tends to occur more frequently on an irrational rather than a rational level, as individuals tend to follow their intuition with little regard to privacy risks.

Attitudes Regarding Online Privacy

Sharing personal information online has become routine and more embedded in everyday social interactions (Zafeiropoulou, Millard, Webber & O'Hara, 2013). Privacy concerns were perhaps more prominent in the early days of the internet, but a rising percentage of people today are less concerned about potential risks due to "a growing internet population, constantly changing areas of use, and increasing security awareness" compared to earlier in the 21st century (Bergstrom, 2015, p. 425). Some internet users are fully aware of the risks they face online, and willingly accept those risks for access to certain services, thus engaging in a cost-benefit analysis (Park, Campbell, & Kwak, 2012; Preibusch, 2013). Consumers have been shown to willingly forego certain online privacy protections to access more customized content (Martin & Murphy, 2017; Sundar, Kang, Wu, Go & Zhang, 2013). It is quite possible that many users experience what Choi, Park, and Jung refer to as "privacy fatigue," an umbrella term for concepts ranging from security fatigue (Furnell & Thompson, 2009), to consent fatigue (Schermer, Custers, & van der Hof, 2014), and breach fatigue (Kwon & Johnson, 2015), in which users experience a "psychological state of tiredness with the issue of online privacy" (2018, p. 43).

It has been shown that people with a more sophisticated apprehension of the internet, who are better able to perceive privacy threats, are no better off than laypersons with respect to acting to secure their privacy online (Kang, Dabbish, Fruchter, & Kiesler, 2015). An over-reliance upon self-reporting studies could account for part of the discrepancy as there is a demonstrated tendency for internet users to be overly confident in their own competence. Jensen, Potts, and Jensen (2005) asked participants if they were familiar with technological solutions to enhance their privacy, and less than 25 percent of participants who answered in the affirmative were able to answer basic follow-up questions about the technology.

Concerns related to online privacy develop from personal experience, and include discussions with friends and family and hearing reports about data breaches through media channels that resulted in financial losses (Brandimarte et al., 2013, Bryce and Fraser, 2014). Simply put, many people may have become inured to the notion of their personal data being exposed online, and may appreciate those risks only after a negative experience. In 2016, there were more than 4,000 data breaches that affected more than 4.2 billion records (Risk-Based Security, 2017). These data breaches, in turn, often result in user information being sold on the dark web (Ablon, Libicki & Golay, 2014).

In the past few years, consumers have become more knowledgeable about the ways in which their data is being used (Morey, Forbath & Schoop, 2015). It has been argued that 2018 is the year in which consumers grew more informed and cynical about the ways in which their personal data is used (Ng, 2018), as a recent poll indicates a majority of Americans reported changing their privacy settings in the past 12 months (Perrin, 2018).

THREATS TO ONLINE PRIVACY

The article examines internet privacy through four complementary and overlapping perspectives: user activity, corporate data collection, governmental surveillance, and malevolent actors. To be sure, user activity is the most important factor, as a more established and connected online presence generally makes one more susceptible to having private information accessed without their consent or knowledge. At the same time, data collection by governments and corporate entities, as well as the activities of malevolent actors pose significant threats to user privacy. The primary focus is on the United States, as an endeavor to include other nation-states would inevitably exclude some populations while also sacrificing a more in-depth discussion of privacy.

User Activity

Certain individuals increase their vulnerability to being a victim of an online scam. A recent survey of more than 11,000 internet users demonstrated that weak self-control—by way of willingness to engage in risky investments—in addition to relatively mundane internet tasks, i.e. online shopping and opening emails from unknown sources, were factors that increased the likelihood of falling victim to online schemes (Chen et al., 2017). Aside from those relatively risky behaviors, more routine online actions can pose threats to a user's information privacy. The remainder of this section examines apps, Facebook, and the Internet of Things.

Apps

In 2019, smartphones are expected to eclipse TV as the popular medium, with adult users spending more than 215 minutes each day on their mobile devices—and 90% of that time on apps (Wurmser, 2018).

There had been a variety of anecdotal reports regarding the amount of data that apps collected on users. Personal injury law firms have sent advertisements to the phones of patients—and others—sitting in emergency rooms (Allyn, 2018). The CEO of Moviepass recently noted, “We watch how you drive from home to the movies. We watch where you go afterwards” (Fussell, 2018, n.p.).

An investigative report by *The New York Times* revealed that apps gathered a user's location information “as often as every two seconds,” and that more than 75 companies receive granular location data—often from local news and weather apps—with location accuracy within a few yards, and coordinates that are “in some cases updated more than 14,000 times a day” (Valentino-DeVries, Singer, Keller & Krolik, 2018).

Facebook

Facebook is the most popular social media platform in the U.S., with more than two-thirds of Americans having an account, and 75 percent of those users accessing the platform daily (Smith & Anderson, 2018). The more an individual uses various social media platforms, “the more overlapping, cross-referenced data” points are provided, since larger platforms buy or develop emerging platforms, “like how Facebook bought Instagram and WhatsApp, so they all connect data sets” (McKew, 2018, n.p.) This is potentially at odds with the expectation by consumers that popular platforms, e.g., Facebook and Twitter, should be the most adept at protecting sensitive information (Luttrell, 2019).

Advertisers have moved beyond using Cookies to using digital fingerprints from browsers, with some companies examining punctuation and tone in emails to establish personality profiles, while Facebook

has developed more than 50,000 attributes by which to categorize its users (Angwin, Mattu, & Parris, 2016). As Zeynep Tufekci (2018) put it: “What Facebook does is profile you. If you’re on Facebook, it’s collecting everything you do. If you’re off Facebook, it’s using tracking pixels to collect what you’re browsing. For its microtargeting to work, for its business model to work, it has to remain a surveillance machine” (Jacoby, 2018).

One component of Facebook, the “People You May Know” feature, is designed to allow users to add people to their social network. The feature relies on an algorithm that looks at a user’s friend list, education and work information, and their friends-of-friends, but also address books, work email addresses, and—despite public claims to the contrary—locations and IP addresses to make friend recommendations (Hill, 2018a). Facebook has also used targeted ads with information that was not directly provided by or revealed to users, and those users remain unable to view or delete their information, or even prevent advertisers from using their data (Hill, 2018b).

Facebook executives were questioned by members of Congress about the company’s privacy policies following the Cambridge Analytica scandal that exposed the personal information of more than 50 million users. In short, a personality profile app that was designated for academic use harvested information from individuals who took the survey—as well as information from their friends’ profiles—without their knowledge (Granville, 2018). This was, in essence, a hidden usage of public data whereby user information migrated from the clear web to the deep web.

The continued negligence by Facebook in taking adequate action to prevent additional breaches of security has resulted in a potential fine of \$1.63 billion under new E.U. privacy laws (Schechner, 2018). In December 2018, the British Parliament released internal documents from Facebook showing the company collected call records and text messages without user permission (Kirka, Bajak, & Ortutay, 2018). Company emails showed the move was acknowledged as “a pretty high-risk thing to do from a PR perspective” (Satariano & Isaac, 2018). The documents also revealed that Facebook white-listed certain companies such as Airbnb, Lyft, and Netflix, giving them preferred access to consumer data that other companies were not allowed to access following a policy change.

A recent Pew Research study following the Cambridge Analytica scandal showed that 42 percent of Facebook users had “taken a break” from the platform in the past 12 months, while 26 percent deleted the app from their phone altogether (Perrin, 2018).

Internet of Things

The Internet of Things (IoT) refers to everyday objects being able to send and receive data through the internet. Verizon estimates there will be 30 billion IoT devices by 2020—more than triple the number of devices in 2014; the “potential value generated” by IoT in 2025 ranges from \$3.9 trillion to \$11.1 trillion (Jalali, Kaiser, Siegel & Madnick, 2017, p. 3). Ownership of that data is complex, as data is generated by a user’s actions and could be considered theirs, but is produced and analyzed by the manufacturer of the product (Saarikko, Westergren, & Blomquist, 2017).

The appeal of IoT devices revolves around convenience and improving daily life (Green, 2017). At the same time, these sensing devices have been characterized as posing “an unprecedented threat to individual privacy,” as users “become targets of data collection without even noticing it and in hitherto unsuspected situations” (Lopez, Rios, Bao & Wang, 2017, p. 47). The authors concluded that legal protections against privacy intrusions on such devices remain limited. This is troubling given that IoT’s “security track record has been extremely poor,” as many devices lack the ability to be patched, leaving

them “permanently at risk,” and that problem is expected to become “more widespread and intractable” as the cost of making a device “smart” (Ranger, 2018, n.p.).

Such data is typically stored via cloud computing, where individuals and organizations store data on servers owned by third parties which may have “different agendas, responsibilities and vulnerabilities” and therefore “adds another layer of complexity” (Kernighan, 2017, p. xii). Furthermore, because personal data is frequently transmitted beyond the country of origination, it has been posited that “data havens could emerge similar to tax havens” whereby firms are able to store data in parts of the world with diluted privacy regulations (Newman, 2015, p. 508). The public cannot readily access this collection of IoT data, and that opacity is emblematic of information on the deep web.

Viewed holistically, what many people might view as routine activities—checking the weather, logging into the Facebook account, setting a timer through a home assistant like Alexa or Google Home, or simply walking around with a smartphone in their pocket—all function to generate a highly detailed view of consumer behavior. These user activities therefore frequently overlap and interact with corporate interests in acquiring consumer data.

CORPORATE DATA COLLECTION

There is growing corporate interest in Big Data, a trend that dates back to 2011 (Burrows & Savage, 2014). While there is no agreed-upon definition of Big Data, the National Bureau of Economic Research identified “new” aspects of it as data being “available faster, [with] greater coverage and scope, and includes new types of observations and measurements that previously were not available,” with “less structure, or more complex structure” than traditional data sets (Einav & Levin, 2014, p. 3).

Businesses frequently acquire and store consumer data before determining how to use the data that is being collected (Mayer-Schonberger & Cukier, 2013). Similarly, marketing practices that use consumer data have outpaced academic scholarship on the subject (Martin & Murphy, 2017). Data brokers acquire, store and sell consumer data. The FTC examined the databases of data brokers and found one had information regarding 1.4 billion consumer transactions, another had information on more than \$1 trillion in consumer transactions, another adds three billion new records each month, and a final data broker had “3,000 data segments for nearly every U.S. consumer” (Ramirez, Brill, Ohlhausen, Wright & McSweeney, 2014, p. iv).

In 2017, Congress repealed regulations that prevented internet service providers from selling personal information, giving those companies “free rein to do what they like with your browsing history, shopping habits...location, and other information” while also preventing the FCC from establishing privacy protections in the future (Wheeler, 2017). The editorial board of *The New York Times* argued that without stronger privacy regulations, more sophisticated users might rely upon virtual private networks and other privacy-enhancing tools, but “most Americans are unlikely to be conversant with such tricks of the trade” (2017).

European consumer groups have filed complaints alleging that Google used “deceptive design and misleading information which results in users accepting to be constantly tracked,” as it tracked, collected and aggregated users’ movements (Porter, 2018, n.p.). This follows a lawsuit in the U.S. that accused the search engine of tracking the location of smartphones even when the location history of the phone was turned off (Farivar, 2018).

Finally, in what could be possibly described as malevolent action by digital companies, there have been mainstream media reports that gather anecdotes from users who believe smartphone devices have

recorded their offline conversations (Langone, 2018; Hill, 2017). Whereas some vocal triggers, e.g., “Hey Siri,” will activate a microphone, Facebook and Instagram are thought to have thousands of potential triggers that would periodically allow the platform to access a user’s microphone (Nichols, 2018).

GOVERNMENT SURVEILLANCE

In the month following the terrorist attacks on September 11, 2001, the U.S. federal government passed The USA PATRIOT Act of 2001 in an effort to enhance national security. The sweeping legislative act expanded the ways in which federal agencies could monitor the communication of citizens. Law enforcement officials could now legally track email and internet usage without meeting a probable cause requirement (Lee, 2003). While many provisions of the Act initially had sunset clauses that aided its initial passage, Congress has subsequently extended the vast majority of those elements that were set to expire, and those surveillance tools remain in use today.

In 2013, Edward Snowden, a contractor working for the National Security Agency, illegally leaked classified information that revealed the existence of various global surveillance programs operated by the NSA and other governmental agencies, and aided by telecommunication companies. The “scale, reach, and technical sophistication” of this surveillance was unknown to the general public, and “came as a surprise even to seasoned observers” (Bauman, et al., 2014, p. 122). The NSA required Verizon to deliver metadata from the phone calls of millions of Americans, and Verizon was instructed to disclose neither the order nor the request for those records; furthermore, the PRISM program gave the NSA direct access to the servers of Apple, Facebook, Google, Microsoft, Skype, Yahoo, and YouTube—with those companies assisting the government in its efforts (Lyon, 2014).

The information revealed by Snowden generated a sense of distrust toward intelligence agencies not only in the United States but other nations in the “Five Eyes”—Australia, Canada, New Zealand, and the United Kingdom—and elsewhere in Europe (Walsh & Miller, 2016). In addition to the clear implications for user privacy, the exposure of these programs was shown to have had a chilling effect on search patterns (Marthews & Tucker, 2017), the use of Wikipedia (Penney, 2016) as well as the expression of marginalized political viewpoints (Stoycheff, 2016).

MALEVOLENT ACTORS

Perhaps the most overt and obvious threat to personal privacy—not to mention the biggest financial risk for users—are malevolent actors.

Russian hackers were indicted for their attempts to influence the 2016 U.S. presidential election. There, hackers who have been caught by the government are often given the choice of going to jail or working for the Russian state (Matthews, 2015). It is believed that many governments will continue to recruit more cyber-criminals in the future, as rogue hacker operations are uncovered, with an expert arguing that “it would be no surprise if there are links, and it would be a great surprise if there were no links” between such criminals and state actors (McGuffin, 2018, n.p.).

North Korean hacking groups have engaged in the online theft of more than \$100 million, the majority of which came from the central bank of Bangladesh (Reints, 2018). The U.S. intelligence community has stated that adversaries had the ability to threaten critical infrastructure, as well as IoT devices (Ranger, 2018).

Malevolent actors target social media platforms as well. In April 2018, Facebook announced that “malicious actors” had scraped information from the public profiles of “most” of its 2 billion users, but didn’t disclose the identity of the actors, how data might have been used, or the precise number of people affected (Timberg, Romm & Dwoskin, 2018).

A recent trend by hackers is to engage in real estate wire transfer fraud. A hacker will typically send a phishing attempt to a real estate or title agent. If the agent clicks the link, the hacker is able to view emails and wait for an upcoming sale. The hacker then emails the client directly from the agent’s account with instructions to wire the funds to a fraudulent account—with no legal recourse for the client (Stevens & Dujanovic, 2018).

SOLUTIONS AND RECOMMENDATIONS

Some users may be of the belief that utilizing Private Browsing Mode allows them to navigate online spaces without fear of divulging personal data, yet it has been shown that such browser settings may still reveal private information about the user (Liou, Logapriyan, Lai, Pareja, & Sewell, 2016). Such features protect a user’s browsing history from those who have access to the device, but do not prevent online data tracking (Verger, 2018).

Google allows users to view the activity that has been archived by the company. Users can then “filter by date & product” to view, for example, all of the voice interactions with Google Home and other devices (“My Activity,” n.d.). Facebook users are able to view advertisers that target them by navigating to “Settings > Account Settings > Ads > Advertisers You’ve Interacted With and then check out the section called ‘Advertisers who uploaded a contact list with your info’” (Horaczek, 2018).

The Tor Browser has prioritized user privacy, and operates in a slightly more decentralized fashion than a virtual private network. While the browser was considered to be usable only by relatively sophisticated users, a September 2018 update revamped the user interface, making it more inviting to a broader base of users (Nield, 2018). Even some of the most sophisticated users who combine a TOR browser with a Virtual Private Network connection to a reliable provider do not enjoy complete privacy protection, as users of TOR have had their identities revealed, and “VPN providers aren’t necessarily beyond the reach of law enforcement” (Mathews, 2017).

The Electronic Frontier Foundation, a nonprofit digital rights group, has established a webpage for users, who—with a single click—can determine how well their existing browser blocks online trackers (“Panopticklick 3.0,” n.d.). It also created a free Privacy Badger plugin, which blocks invisible trackers that pass through most popular web browsers (“Privacy Badger,” n.d.). The search engine DuckDuckGo does not track users, and has taken the stance that “The internet shouldn’t feel so creepy and getting the privacy you want online should be as simple as closing the blinds” (“Welcome to,” n.d.). The privacy-friendly search engine experienced record-high usage in 2018, due in large part to highly publicized data breaches (Lacy, 2018).

The Mozilla Foundation generated a list of dozens of common IoT devices, assigning them an aggregate score of “not creepy,” “a little creepy,” “somewhat creepy,” “very creepy,” or “super creepy,” based on what the device knows about the user, the degree of user control, the company’s responsiveness to consumers, and potential worst-case scenarios (“Privacy not included,” n.d.).

FUTURE RESEARCH DIRECTIONS

The Privacy Paradox has been explored a fair amount in recent years, with Barth and de Jong (2017) suggesting that it may be time to bifurcate online privacy research between stationary online use and mobile use. Future studies should consider that self-reports on privacy practices tend to be unreliable, particularly when accounting for events that are infrequent, so actual evidence of particular behaviors rather than self-reports is likely to yield the most insight into consumer behaviors (Kokolakis, 2017).

Perhaps another path forward in Privacy Paradox studies is to develop a standardized baseline for consumer privacy protection behavior. There may be a chasm between what an online user considers to be reasonable privacy precautions--perhaps through inaction, e.g., not responding to blatant phishing attempts, or avoiding websites that browsers mark as “unsafe” --and what researchers would characterize as proactive privacy protection measures.

Organizations could undertake efforts to clarify and simplify the terms and conditions for consumers using their websites and apps. Aside from ethical considerations, there are financial incentives for companies to embrace consumer privacy. Recent research demonstrates that firms which prioritize the privacy of consumers in a way that is deemed “authentic” will reap benefits including a “favorable market response, customer loyalty, and engagement” (Martin & Murphy, 2017, p. 152).

In terms of potential legislative remedies, the United States has a system described as “fragmented” and “patchwork” with “stronger protections for video rentals than online marketing, and lacking a regulatory body capable of dealing with present-day demands for privacy protection (Newman, 2015, p. 507). In light of this, some states have acted to bolster online privacy for users. California passed a law that will take effect in 2020 which grants consumers “the right to know what information companies are collecting...why they are collecting that data and with whom they are sharing it,” as well as giving consumers the right to demand that companies delete or not share their information without it impacting the quality of service provided by the company (Wakabayashi, 2018, B1).

CONCLUSION

The disclosure of a company’s privacy policy is viewed as an alternative to government regulation (Reidenberg, Breau, Carnor, & French, 2015). But it is not reasonable to expect consumers to read the privacy policy of each website they visit, as the time it would take to do so exceeds the total amount of time people spend online (McDonald & Cranor, 2008). In short, “something isn’t quite right with the whole system” and “shifting more of the responsibility to the websites who profit off your data might be a good way to start fixing it” (Wagstaff, 2012).

There has been a noted “creepy factor” of collecting personal information, as many consumers consider it an invasion of privacy (Kshetri, 2014, p. 1137) and users have described themselves as feeling “unsettled knowing their every click and ‘like’ is tracked, quantified—and sold” (Zomorodi, Poyant, & Aaron, 2017). Indeed, the confluence of digital technologies and Big Data has been referred to as “uncontrolled electronic panopticism” (Smith & Kollars, 2015, p. 160).

A bit of good news is that people who have fallen victim to an internet scam are more likely to build knowledge about the potential severity of the issue, and take account of the online spaces in which they remain vulnerable to further attack (Chen et al., 2017; Mohamed & Ahmad, 2012).

The future of internet privacy in the era of Big Data is uncertain, though there is a reasonable cause for concern. China has unveiled a social credit system that combines bank account information, court

records, and internet search history, combined with facial recognition, gait analysis and voice recognition with the stated goal of “allow[ing] the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step” (Chun, 2018, n.p.). Meanwhile, India has a biometric database, Aadhaar, that contains digital identities with fingerprints and iris scans of more than one billion residents, though it has proven vulnerable to hacking as well as more mundane security breaches, as a group of journalists were given full administrative access to the database for less than \$10 (Cameron, 2018).

The risks to individual privacy online are greater today than they were 10 years ago, and those risks are likely to increase in the years ahead as more users—consciously or unwittingly—become more connected through apps, social media platforms, and the Internet of Things. The information age was once thought to characterize a knowledge-based society, but it may also come to be viewed as characterizing the behavior of corporate entities and malevolent actors who are driven to generate and extract private data from members of that society.

REFERENCES

- Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Rand Corporation.
- Allyn, B. (2018, May 25). Digital ambulance chasers? Law firms send ads to patients' phones inside ERs. *NPR*. Retrieved from <https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers>
- An attack on internet privacy. (2017, March 28). *The New York Times*, p. A26.
- Angwin, J., Mattu, S., & Parris, T., Jr. (2016, December 27). Facebook doesn't tell users everything it really knows about them. *ProPublica*. Retrieved from <https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. doi:10.1016/j.tele.2017.04.013
- Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 2(8), 121–144. doi:10.1111/ips.12048
- Bergstrom, A. (2013). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419–426. doi: 0747-5632/doi:10.1016/j.chb.2015.07.025
- Brandimarte, L., Acquisti, A., & Lowenstein, G. (2013). Misplaced confidences, privacy, and the control paradox. *Social Psychological & Personality Science*, 4(3), 340–347. doi:10.1177/1948550612455931
- Brown, B. (2001). *Studying the internet experience*. HP Laboratories Technical Report HPL-2001-49. Retrieved from <http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf>
- Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young people's online interactions. *Computers in Human Behavior*, 30, 299–306. doi:10.1016/j.chb.2013.09.012

Burrows, R. & Savage, M. (2014, April). After the crisis? Big data and the methodological challenges of empirical sociology. *Big Data & Society*, 1-6.

Cameron, D. (2018, September 11). Simple hack turns India's massive biometric database into a profitable counterfeit system. *Gizmodo*. Retrieved from <https://gizmodo.com/simple-hack-turns-indias-massive-biometric-database-int-1828972521>

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291–302. doi:10.1016/j.chb.2017.01.003

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 8, 42–51. doi:10.1016/j.chb.2017.12.001

Chun, R. (2018, April). China's new frontiers in dystopian tech. *The Atlantic*. Retrieved from <https://www.theatlantic.com/magazine/archive/2018/04/big-in-china-machines-that-scan-your-face/554075/>

Einav, L., & Levin, J. (2014). The data revolution and economic analysis. *National Bureau of Economic Research*, 14, 1-24. Retrieved from <https://www.nber.org/chapters/c12942.pdf>

Farivar, C. (2018, August 20). Man sues over Google's "location history" fiasco, case could affect millions. *Ars Technica*. Retrieved from <https://arstechnica.com/tech-policy/2018/08/did-google-violate-users-privacy-when-it-secretly-kept-location-data/>

Furnell, S., & Thompson, K. L. (2009). Recognising and addressing 'security fatigue.'. *Computer Fraud & Security*, 11(11), 7–11. doi:10.1016/S1361-3723(09)70139-3

Fussell, S. (2018, March 5). Moviepass CEO brags app tracks your location before and after movies. *Gizmodo*. Retrieved from <https://gizmodo.com/moviepass-ceo-brags-app-tracks-your-location-before-and-1823525088>

Granville, K. (2018, March 19). Facebook and Cambridge Analytica: What you need to know as fallout widens. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

Green, H. (2016, Oct. 4). How the Internet of Things will change (and improve) our everyday lives. *Forbes*. Retrieved from <https://www.forbes.com/sites/ibm/2016/10/04/how-the-internet-of-things-will-change-and-improve-our-everyday-lives/#712ec725374b>

Hill, K. (2018a, August 8). 'People you may know:' A controversial Facebook feature's 10- year history. *Gizmodo*. Retrieved from <https://gizmodo.com/people-you-may-know-a-controversial-facebook-features-1827981959>

Hill, K. (2018b, September 26). Facebook is giving advertisers access to your shadow contact information. *Gizmodo*. Retrieved from <https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051>

Hill, S. (2017, January 15). Is your smartphone listening to everything you say? We asked the experts. *Digital Trends*. Retrieved from <https://www.digitaltrends.com/mobile/is-your-smartphone-listening-to-your-conversations/>

Horaczek, S. (2018, April). You wanna see something wild? Check out all the advertisers targeting you on Facebook. *Popular Science*. Retrieved from <https://www.popsci.com/advertisers-targeting-facebook-account-settings>

Jacoby, J. (2018). *The Facebook Dilemma*. Public Broadcasting Service.

Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2017). *Internet of Things (IoT) promises new benefits—and risks: A systematic analysis of adoption dynamics of IoT products*. Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. Working Paper CISL#2017-15. Retrieved from <http://web.mit.edu/smadnick/www/wp/2017-15.pdf>

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of internet users: Self- reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2), 203–227. doi:10.1016/j.ijhcs.2005.04.019

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). “My data just goes everywhere”: User mental models of the internet and implications for privacy and security. *Eleventh Symposium on Usable Privacy and Security*, 39-52. Retrieved from <https://www.usenix.org/system/files/conference/soups2015/soups15-paper- kang.pdf>

Kernighan, B. W. (2017). *Understanding the digital world: What you need to know about computers, the internet, privacy, and security*. Princeton, NJ: Princeton University Press.

Kirka, D., Bajak, F., & Ortutay, B. (2018, December 5). Documents show Facebook used user data as competitive weapon. *Associated Press*. Retrieved from <https://www.apnews.com/f15fe5b986ba4426b-4f3267e8e1322f0>

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. doi:10.1016/j.cose.2015.07.002

Kshetri, N. (2014). Big data’s impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38(11), 1134–1145. doi:10.1016/j.telpol.2014.10.002

Kwon, J., & Johnson, M. E. (2015). *The market effect of healthcare security: Do patients care about data breaches?* Paper presented at the workshop on the economics of information security (WEIS 15). Retrieved from <https://pdfs.semanticscholar.org/f3c4/2d80583f5d87957a9dbd8bf0bdd4db3c279d.pdf>

Lacy, L. (2018, December 3). DuckDuckGo is shedding its black sheep status thanks to its dedication to privacy. *AdWeek*. Retrieved from <https://www.adweek.com/digital/duckduckgo-is-shedding-its-black-sheep- status-thanks-to-its-dedication-to-privacy/>

Langone, A. (2018, March 30). Here’s how Facebook or any other app could use your phone’s microphone to gather data. *Time*. Retrieved from <http://time.com/money/5219041/how-to-turn-off-phone-microphone-facebook- spying/>

Lee, L. T. (2003). The USA PATRIOT Act and telecommunications: Privacy under attack. *Rutgers Computer & Technology Law Journal*, 29, 371.

Liou, J. C., Logapriyan, M., Lai, T. W., Pareja, D., & Sewell, S. (2016). A study of the internet privacy in private browsing mode. *Proceedings of the 3rd multidisciplinary international social networks conference*, 1-7. 10.1145/2955129.2955153

Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems*, 75, 46–57. doi:10.1016/j.future.2017.04.045

Luttrell, R. (2019). *Social Media: How to engage, share, and connect* (3rd ed.). London, UK: Rowman & Littlefield.

Lyon, D. (2014). *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*. Big Data & Society. doi:10.1177/2053951714541861

Marthews, A., & Tucker, C. E. (2017). *Government surveillance and internet search behavior*. Available at SSRN 2412564

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. doi:10.1007/11747-016-0495-4

Mathews, L. (2017, January 27). What is private browsing and why should you use it? *Forbes*. Retrieved from <https://www.forbes.com/sites/leemathews/2017/01/27/what-is-private-browsing-and-why-should-you-use-it/#74686e4e25b1>

Matthews, O. (2015, May 7). Russia's greatest weapon may be its hackers. *Newsweek*. Retrieved from <https://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html>

Mayer-Schonberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think*. Boston, MA: Houghton Mifflin Harcourt.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4, 543–568.

McKew, M. (2018, March 19). What *everyone* needs to know about the Facebook data breach. *Cosmopolitan*. Retrieved from <https://www.cosmopolitan.com/politics/a19484431/molly-mckew-facebook-instagram-youtube-manipulating-your-mind/>

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366–2375. doi:10.1016/j.chb.2012.07.008

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, 93, 96–105. Retrieved from https://s3.amazonaws.com/academia.edu.documents/49352349/CUSTOMER_DATA-DESIGNING_FOR_TRANSPARENCY_AND_TRUST-R1505H-PDF-ENG.desbloqueado.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1543964166&Signature=52Ri0jn1cWtDJmP%2Fv21vjvzUPu8%3D&response-content-disposition=inline%3B%20filename%3DCustomer_Data_Designing_for_Transparency.pdf

My Activity. (n.d.). *Google*. Retrieved from <https://myactivity.google.com/myactivity>

Newman, A. L. (2015). What the “right to be forgotten” means for privacy in a digital age. *Science*, 347(6221), 507–508. doi:10.1126/science.aaa4603 PMID:25635090

Ng, A. (2018, December 7). Tech's invasion of our privacy made us more paranoid in 2018. *CNET*. Retrieved from <https://www.cnet.com/news/techs-invasion-of-our-privacy-made-us-more-paranoid-in-2018/>

Nichols, S. (2018, June 4). Your phone is listening and it's not paranoia. *Vice*. Retrieved from https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia

Nield, D. (2018, September 7). The super-private Tor Browser gets a huge update, but should you switch from Chrome? *Gizmodo*. Retrieved from <https://gizmodo.com/the-super-private-tor-browser-gets-a-huge-update-but-s-1828879886>

Norberg, P. A., Horned, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, 41(1), 100–126. doi:10.1111/j.1745-6606.2006.00070.x

Oremus, W. (2018, April). Are you really the product? The history of a dangerous idea. *Slate*. Retrieved from <https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html>

Panopticlick 3.0. Is your browser safe from tracking? (n.d.). *Electronic Frontier Foundation*. Retrieved From <https://panopticlick.eff.org/>

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, 28(3), 1019–1027. doi:10.1016/j.chb.2012.01.004

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, 31, 117.

Perrin, A. (2018, September 5). Americans are changing their relationship with Facebook. *Pew Research Center*. Retrieved from <http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>

Porter, J. (2018, November 27). Google accused of GDPR privacy violations by seven countries. *The Verge*. Retrieved from <https://www.theverge.com/2018/11/27/18114111/google-location-tracking-gdpr-challenge-european-deceptive>

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71(12), 1133–1143. doi:10.1016/j.ijhcs.2013.09.002

Privacy Badger. (n.d.). *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/privacybadger/faq>

Privacy not included. (n.d.). *Mozilla Foundation*. Retrieved from <https://foundation.mozilla.org/en/privacynotincluded/>

Ramirez, E., Brill, J., Ohlhausen, M. K., Wright, J. D., & McSweeney, T. (2014). Data brokers: A call for transparency and accountability. *Federal Trade Commission*. Retrieved from <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>

Ranger, S. (2018, August 21). What is the IoT? Everything you need to know about the Internet of Things right now. *ZDNet*. Retrieved from <https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/>

Reidenberg, J. R., Breaux, T., Carnor, L. F., & French, B. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, 30(1), 39–88. doi:10.15779/Z384K33

Reints, R. (2018, October 3). “Active and dangerous” North Korean hacking group is behind theft of \$100 million, security firm warns. *Fortune*. Retrieved from <http://fortune.com/2018/10/03/north-korea-hacking-apt38/>

Risk-Based Security. (2017, January). *Data Breach QuickView 2016*. Retrieved from <https://pages.riskbasedsecurity.com/2016-ye-breach-quickview>

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. doi:10.1080/00223980.1975.9915803 PMID:28136248

Rosenberg, R. (1992). *The social impact of computers*. San Diego, CA: Academic Press.

Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? *Business Horizons*, 60(5), 667–676. doi:10.1016/j.bushor.2017.05.010

Satariano, A., & Isaac, M. (2018, December 5). Facebook's emails tell a cutthroat tale. *The New York Times*, p. B1.

Schechner, S. (2018, September 30). Facebook faces potential \$1.63 billion fine in Europe over data breach. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906>

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, 16(2), 171–182. doi:10.1007/10676-014-9343-8

Smith, A., & Anderson, M. (2018, March 1). Social media use in 2018. *Pew Research Center*. Retrieved from <http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>

Smith, E. J., & Kollars, N. A. (2015). QR panopticism: user behavior triangulation and barcode-scanning applications. *Information Security Journal: A Global Perspective*, 24(4-6), 157-163.

Smith, H. J., Milberg, J. S., & Burke, J. S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *Management Information Systems Quarterly*, 20(2), 167–196. doi:10.2307/249477

Stevens, M., & Dujanovic, D. (2018, October 26). Homebuyers targeted by sophisticated, billion dollar hacking scheme. *KSL*. Retrieved from <https://www.ksl.com/article/46414717/homebuyers-targeted-by-sophisticated-billion-dollar-hacking-scheme>

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly*, 93(2), 296–311. doi:10.1177/1077699016630255

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013, April). Unlocking the privacy paradox: do cognitive heuristics hold the key? In CHI '13 extended abstracts on human factors in computing systems (pp. 811-816). doi:10.1145/2468356.2468501

Timberg, C., Romm, T., & Dwoskin, E. (2018, April 4). Facebook: 'Malicious actors' used its tools to discover identities and collect data on a massive global scale. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.0cf79dfa7abf

Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your apps know where you were last night, and they're not keeping it secret. *The New York Times*, Retrieved from <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?mtrref=www.google.com&linked=google>

Wagstaff, K. (2012, March 6). You'd need 76 work days to read all your privacy policies each year. *Time*. Retrieved from <http://techland.time.com/2012/03/06/you-d-need-76-work-days-to-read-all-your-privacy-policies-each-year/>

Wakabayashi, D. (2018, June 28). California passes major online privacy law. *The New York Times*, p. B1.

Walsh, P. F., & Miller, S. (2016). Rethinking 'Five Eyes' security intelligence collection policies and practice post Snowden. *Intelligence and National Security*, 31(3), 345–368. doi:10.1080/02684527.2014.998436

Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. doi:10.2307/1321160

Welcome to DuckDuckGo. (n.d.). Retrieved from <https://duckduckgo.com/about>

Wheeler, T. (2017, March 28). The G.O.P. just sold your privacy. *The New York Times*, p. A27.

Wurmser, Y. (2018, June 18). Mobile time spent 2018. *eMarketer*. Retrieved from <https://www.emarketer.com/content/mobile-time-spent-2018>

ADDITIONAL READING

Akerlof, G. A., & Shiller, R. J. (2015). *Phishing for phools: The economics of manipulation and deception*. Princeton University Press.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147–154. doi:10.1016/j.chb.2015.11.022

boyd, d., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, 15(5), 662–679. doi:10.1080/1369118X.2012.678878

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42–51. doi:10.1016/j.chb.2017.12.001

Doctorow, C. (2018, March 20). Yet another lesson from the Cambridge Analytica fiasco: Remove the barriers to user privacy control. Electronic Frontier Foundation. Retrieved from <https://www.eff.org/deeplinks/2018/03/why-we-didnt-make-fix-my-facebook-privacy-settings-tool>

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, 54(7), 948–957. doi:10.1016/j.im.2017.02.004

Lee, T., Pappas, C., & Perrig, A. (2018). Bootstrapping privacy services in today's internet. *Computer Communication Review*, 48(5), 1–9. Retrieved from https://netsec.ethz.ch/publications/papers/ccr18_pd.pdf

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2017). The role of privacy concerns in the sharing economy. *Information Communication and Society*, 21(10), 1472–1492. doi:10.1080/1369118X.2017.1339726

Trepte, S., Teutsch, D., Masure, P. K., Eicher, C., Fischer, M., Hennhofer, A., & Lind, F. (2014). Do people know about privacy and data protection strategies? Toward the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European Data Protection Law. Law, Governance and Technology Series*, 20. Dordrecht: Springer.

Turow, J., Hennessy, M., & Draper, N. (2018). Persistent misperceptions: Americans' confidence in privacy policies, 2003-2015. *Journal of Broadcasting & Electronic Media*, 62(3), 461–478. doi:10.1080/08838151.2018.1451867

Verger, R. (2018, June 5). What you need to know about your browser's digital fingerprints, *Popular Science*, Retrieved from <https://www.popsoci.com/what-are-digital-fingerprints>

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013, May). Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? In *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 463-472). 10.1145/2464464.2464503

Zomorodi, M., Poyant, J., & Aaron, K. (2017, January 30). Privacy paradox: What you can do about your data right now. *NPR*, Retrieved from <https://www.npr.org/sections/alltechconsidered/2017/01/30/512434746/privacy-paradox-what-you-can-do-about-your-data-right-now>

KEY TERMS AND DEFINITIONS

4

Big Data: A data set this is too large for “standard” software programs, and is generally used to identify large trends, and predict behaviors and outcomes.

Cloud Computing: The use of remote servers via the internet—rather than a local server or personal computer—to store and process data.

Cookies: Small text files that are placed on a user’s web browser as they visit a website.

Data Breach: An incident where information is accessed without authorization.

Internet of Things: A network of physical objects embedded with sensors that enable them to collect and share data.

Phishing: An attempt to obtain a user’s sensitive data through the use of a fraudulent identity via electronic communication.

Privacy Paradox: Individuals often claim to be concerned about threats to their privacy, yet do not act to protect their personal information.

Private Browsing Mode: A privacy feature in web browsers that disables a user’s browser and search history.

Protection Motivation Theory: This concept attempts to explain the way in which individuals react to perceived threats, and holds that individuals consider the perceived severity and probability of a threat, as well as the efficacy of their potential response.

Virtual Private Network: A technology that uses an encrypted connection to add security and privacy to private and public networks.

Societal Safety and Preservation in the Digital Era

Dylas Gudoshava

Zimbabwe Open University, Zimbabwe

INTRODUCTION

Personal privacy is being eroded from various directions as modern technologies bring numerous threats towards personal privacy. People are often unconscious about it and accept violation of privacy to a great extent without questions. Technological advancement has been embraced by all nations including developing countries. Today, the world is like a village where people share information at the same time but in different parts of the world over the internet.

Developing countries venture into new technologies without understanding the implications and the legal frame works under which the technologies operate. According to the 40th International Conference of Data protection and Privacy commissioners (2019), the technological pace keeps accelerating while the legal pace remains particularly slow. For this reason, developing countries may not effectively deal with crimes committed over the internet or in the office work environment. Spammers for instance, may send spam over the internet with little or no knowledge of users in developing countries. Although these countries may have laws on data protection, these laws are general in character and may not apply in crimes like spamming. Palfrey (2005) explained that, some countries use existing laws of general application to fight crimes like spam. Unfortunately, an observation made in 2005 still stands in 2019 as these laws miss their target.

BACKGROUND

Privacy and security are related, hence go hand in hand. The major difference being between legitimate and illegitimate uses of data. An illegitimate use of data is one that is unauthorised, that is, when data is stolen, altered, or viewed by the wrong party. This is the domain of security, which protects data from being inappropriately accessed, modified, or shared. Legitimate uses of data are those that have been authorised. However, in a discussion of privacy, there are plenty of legitimate data uses that may be problematic or harmful. For example, in countries where companies can collect individuals' data with only nominal notification, requiring users to search for ways to opt out, personal data can be used in ways that people did not expect or knowingly give permission to. This is the domain of privacy, which is broadly concerned with how people control and manage data about themselves. In essence, just because something is legal doesn't mean it is constructive.

Today's Internet age is marked by tremendous technological developments which allow for the collection and processing of an indistinct number of personal data. Before the advancement of technology, these data would have simply elapsed. However, with the advent of limitless capacity to store information, such as the cloud, google drive as well as digital space, there has been an increase in capacity of analysing and processing personal data. Personal information of daily life that is isolated does not necessarily

DOI: 10.4018/978-1-5225-9715-5.ch050

endanger personal privacy, however, put together, all this information allows for the creation of profiles of one's personality and such digital biographies increase vulnerability with regard to a variety of dangers. The right to privacy and the right to data protection have thus become two of the most important fundamental rights of modern society. Developments in the field of privacy require an innovative legal and political framework which can guarantee that the technological implications are correctly understood and regulated accordingly.

The Editorial Board (2017) describe Internet privacy as “involving the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet”. It has to be noted that Internet privacy is a subset of data privacy.

Wheeler (2017) noted that “Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behaviour on a website. PII refers to any information that can be used to identify an individual. Age and physical address alone, for example could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person. Some experts such as Steve Rambam, a private investigator specialising in Internet privacy cases, believe that “privacy no longer exists”. He notes that “Privacy is dead – get over it” (Rambam, 2015).

While illegitimate uses of data must be contested with security, legitimate but harmful uses of data must be interrogated through the lens of privacy preservation

The penetration of Internet throughout the world is bringing an increase in volume of user information online. Developing countries such as those of Africa are included as contributors and consumers of this voluminous information. Concerns have been shown from different parts of the world regarding Internet user privacy and security. For Southern African region, very little is known regarding how Internet users are concerned with their online privacy and security. This chapter aims to compare Internet user awareness and concerns about online privacy and security between users in a developing country and users in a developed country, and to determine any common attitudes and differences between these user groups.

Retreating to one's home, closing an office door, or hanging up a phone may have previously allowed a person to feel a measure of control over who might be listening or watching, but the presence of network-connected devices in private spaces can remove this sense of control and privacy (Rosner and Kenneally, 2017). In an article by Fick and Akwagyiram (2019) in the Nairobi/Lagos Reuters, it was noted that “in Kenya, there is a large and fast growing population of internet users”. At the same time, there are no specific laws or regulations to protect the privacy of those individuals. Recent revelations about British analytics firm Cambridge Analytica, which Facebook says improperly accessed personal data of about 50 million of the social networks users in the 2016 U.S. presidential election, have also touched the African continent.

Fick and Akwagyiram (2019) noted that “Kenya is not alone in Africa, which as a region has clocked the world's fastest growth in internet use over the past decade”. Unlike in Europe and the United States, where data-privacy laws provide a level of protection to consumers, many Africans have little or no recourse if a data breach occurs because often legal and regulatory safeguards don't exist. In an article by Kshetri (2019), he observed that there were 24 million malware incidents that targeted Africa in 2016. In a survey conducted in Ghana, it was noted that “in 2016, Ghana's financial institutions were reported to experience more than 400,000 incidents related to malware, 44 million related to spam emails”.

Some economies in the continent are becoming attractive to cybercriminals, thanks to the high degree of digitisation of economic activities. For instance, 86% of South Africans regularly use online banking services. This proportion is higher than many countries in the Middle East and Turkey.

The chapter seeks to answer research questions that follow:

1. What are the laws that are currently in place (if any) to protect user's online privacy?
2. What are the potential barriers to greater online privacy protections?
3. What measures are available for users to have greater online privacy protection?

The research objectives are:

1. To find out the laws currently in place (if any) to protect user's online privacy;
2. To determine potential barriers to greater online privacy protection; and
3. To determine measure that can be taken by internet users to have greater online privacy protection.

As online privacy has become an issue of concern around the world, findings from this study would be beneficial to the policy makers in developed and above all developing countries. Findings could also result into awareness projects in developing countries that sensitise people by creating awareness and understanding about online privacy risks and their impacts in Internet users' offline lives. To the future author, this chapter provides relevant information on user perception of privacy and security in developing countries.

REVIEW OF LITERATURE

In a study done 4 years ago by Ruhwanya (2015), he noted that "the Internet has shaped the way information is stored, shared and distributed around the world". As mentioned above, today's Internet age is marked by tremendous technological developments which allow for the collection and processing of an indistinct number of personal data. Before the advancement of technology, these data would have simply elapsed. However, with the advent of limitless capacity to store information, such as the cloud, google drive as well as digital space, there has been an increase in capacity of analysing and processing personal data. Over the years the advent of google, personal data is among the main driver of today's Internet world especially the social network sites. Social network sites such as Facebook, Twitter, LinkedIn, blogs and picture sharing sites like Instagram and Flickr are driven by user provided information. It has to be noted that Social networking sites in particular are the biggest source of personal information, often unprotected and publicly available (Yanisky-Ravid, 2014). As the amount of online user information increases, privacy has become an issue of concern. User information is sometimes used in decision-making (Nani et al, 2012): for instance, employers can conduct background checks on potential employees from social network sites and use that information to make hiring decisions. As people share their own personal information, websites do track users' browsing behaviours, from browser cookies sometimes without website users' knowledge or consent (Cranor, 2004). Information which is obtained from tracking user behaviour online is used to profile users as well as provide targeted advertisements by marketing and advertising companies.

The advances of Internet and database technology has led to an increase over information privacy concerns (Chung & Paynter, 2002). Data which is entered into forms or contained in existing databases, can be easily combined with transaction records and records of an individual's every click of a mouse on the Internet. Chung & Paynter (2002) further note that "privacy concerns increase further as data mining tools and services become more widely available". Cookies are now widely used to identify users at a web site, some people consider this to be invasion of privacy.

The user will be prompted for information such as buying preferences, age, gender or even an email address. As an example, If one I buying a book from Amazon.com, one will be prompted to enter email address, billing address and other information. The information will be packaged into a cookie and sent to the user's hard drive, which stores it for later user identification. The user's browser will send the cookie to the web server when the user goes to the same web site. The web server can utilise the information in the cookie to generate customised web pages according to the interests and preferences of the user, hence information about one's movement in a web site can also be stored in a cookie.

The main concern is that all this is done without one's knowledge. By using cookies, businesses can obtain personal information such as buying habits, e-mail address or the portions of web site that were looked at previously. This information can be combined into mailing lists for direct marketing purposes or it can be sold to third parties. James (2000), noted that "America Online shares information about its users with various partners, including companies that do direct mailing and telephone solicitations".

A web bug is another widely used instrument that poses a threat using online tracking technology. Some people find it invasive to their privacy when they are visiting a web site. Web bugs are invisible pieces of code that can be used for several purposes, from secretly tracking people's web travels, to pilfering computer files (Stefanie, 2001). The simplest form of web bug is a small graphic interchange format that can work and match with cookies to send information to third parties about a visitor's online travels. An executable bug can install a file onto people's hard drives to collect information whenever they are online. A script-based executable bug can be installed on a user's computer that can take any document from the user's computer without notice. Another form of script-based executable bug is based on servers. They can track visitor's travels on the web and control the person's computer from its server. For example, it launches multiple browser windows when a person tries to exit the site. Many web sites and net advertising companies place web bugs on their pages to collect information, such as which pages are being read most often (Stefanie, 2001). As mentioned earlier, the bugs can be used in a more invasive way, for example, to capture a visitor's Internet Protocol address or installing pernicious files in the visitor's hard drive. The concern is that with a web bug, the visitor's computer can be fully exposed to malicious sites that can take any files or information from programs on the visitor's hard drive without their knowledge and consent.

A report shows that 16 million pages out of 51 million that were scanned contain at least one web bug that had been attached from a third party, such as an advertising network (Stefanie, 2001). When web bugs are used maliciously, the computer user's entire e-mail address book can be stolen without notice merely by clicking on a bugged web page.

Another privacy concern is that marketers can match their customer databases with the databases they get from the cookies. DoubleClick had already built up a database of online consumers' browsing habits by using cookies. It paid Abacus Direct Corporation. \$1.7 billion for the list of catalogue purchasers' names and addresses (Cattapan, 2000). This allows cross-referencing that matches information with real world names, addresses and histories of offline mail order purchases (Anstead, 2000). The acquired names and addresses can be linked with the cookies so DoubleClick not only knew where people are online, but where they live, who they are, and their phone numbers. This could be the most comprehensive customer database in the world that can be used for direct marketing purposes.

What Are The Laws Currently in Place (if any) to Protect a User's Online Privacy?

Privacy law refers to the laws that deal with the regulating, storing, and use of personally identifiable information of individuals, which can be collected by governments, public or private organisations, or other individuals. Over the years, online activities have become progressively more public. Part of this is related to online social networks and the blurring of the line between public and private (Vitak, 2012). Not surprisingly, people have started to become aware that they have little expectations of privacy online and are calling out for more privacy protections (Risen, 2015). Only in 2016 was the Electronic Communications Act of 1986 in Australia revisited (Kelly, 2016) in light of new technology, even when advocates have long stated that the language is outdated (Sidbury, 2001).

Access to Information and Protection of Privacy Act (AIPPA) was enforced in 2002 by the Zimbabwean Parliament. AIPPA was inspired by the Canadian Information Legislation. It sought to provide a legal framework for the access and conduct of requesting information from public bodies and privacy as well the regulation of mass media. According to the Act, only citizens of Zimbabwe, permanently residents or holders of temporary employment, residence permit or student permit are eligible to make request (2002). However many critiques such as David Banistar stated that AIPPA is a rather sceptic name for a media suppressing law.

Zimbabwe's constitution enacted in 2013 explicitly recognises the right to privacy (Section 57):-

Every person has the right to privacy which includes the right not to have:

1. Their home, premise or property entered without permission;
2. Their home, premise or property searched;
3. Their possessions seized;
4. The privacy of their communications infringed; or
5. Their health condition disclosed.

In a post by Makokoba, W (2018), he noted that “although the right to privacy is stated in the constitution, Zimbabwe is one country without clear Personal Data Protection law, literally, people's information is liable to wrong use”.

This leads to the second research question.

What Are the Potential Barriers to Greater Online Privacy Protections?

The answers to these questions still do not offer much to the user in terms of privacy management when they are not highly considered to be the frontier discussions. This is so due to the ever evolving technologies. This leads to the question about measures available for user to have greater online privacy protection. This area will be addressed by examining the state of technology today, online platform business models, and potential governmental interests in the state of internet privacy.

What Measures are Available for Users to Have Greater Online Privacy Protection?

This research question will be addressed by briefly looking at the major current privacy laws in both developed and developing countries. In addition, the rules currently governing the institutions involved

with user privacy agreements will be examined. A detailed list of methods that users can employ to protect their own privacy when institutions fail to protect their privacy rights will be drawn up. These methodologies include both technical and social solutions to protecting online privacy.

CHALLENGES

Technological Advancement in Information and Communication Technology

A lot of progress has been made in discovering new knowledge in the field of information and communication technology. Some of the new knowledge and advancements have been used for the wrong reasons. For instance, hackers use their high-tech skills to change, intrude or interfere with computer networks with an intention of destroying information or making some money out of it e.g. a banking fraudulent deal. Bullesbach (2004) notes that, “development and application of new information and communication technologies lead to challenges of data protection”. Although new technologies in developing countries are a positive move to development, planning is necessary before applying new knowledge. Hackers use principles of new technologies. It should be noted that hackers may indeed be consultants in the particular firms they are working for. It means that such crimes may go undetected or can be detected after a long time. The reason is that the consultant (hacker) occupies a position of trust and nobody would suspect any ill motives in his or her operations.

Capron (1996) explains that, most computer crimes are discovered by accident. Capron (1996) identified a case in which employees of a certain city welfare department created a fictitious workforce and programmed the computer to issue pay cheques, which the employees would intercept and cash.

Spamming is a crime that is also linked to technological advancement in the field of information and communication technology. The current explosion of mobile phone communication and cheap email services has attracted a lot of spamming activities. Palfrey (2005) observed that, spam is the preferred delivery mechanism for internet security threats such as viruses which harm computers and phones. The effects of those in developing countries are largely to persuade users to begin to rely on digital communication. A Kenyan lawyer, Mathew Ngugi observed that the massive gains brought by the information age are not perfect (Ngugi, 2005). This clearly illustrates how the economies of developing countries continue to suffer as they apply new technologies.

Developing countries lack specialised personnel who can effectively deal with advanced computer crime. Computer crimes have become more pronounced and more complicated to the police due to expansion of internet communications (Wikipedia, the free encyclopedia, 2006). This challenge is technological in character which can be associated with the curriculum offered to police officers during their training. They have no training based on information technology and that is why an investigation on computer crime is bound to yield no result as the investigator is not well equipped with current technology based investigative procedures. If law enforcement agents like the police detect a computer crime, Capron (1996), observed that “they do not fully understand the complexities of computer related fraud”.

In an article by Rosner and Kenneally (2017) they noted that “When users of a smart device are presented with a full privacy policy at the outset, these long, convoluted contracts often leave consumers with little understanding of what they are consenting to”. They further highlighted that many companies that capture personal data are not even certain about what they will do with this data in the future, reducing users’ ability to be fully informed about potential uses of collected data. The issues are worse off for devices designed for children. This makes it difficult for parents to protect their children’s privacy.

However, it is widely accepted that most people do not read privacy policies. This therefore means that, parents risk making their children's play and behaviour visible to many third parties, and neither they nor their children are likely to be aware of this.

Inappropriate Legislation and Inadequate Internet Regulations

Inappropriate mechanisms to data protection have hampered data protection in developing countries. Laws on data protection and privacy are there but are not specific to the target. General laws such as consumer protection are largely utilised (Palfrey, 2005). Consumer protection is a general term that can imply personal security against physical injury. There are a lot of inadequacies in the Zimbabwean legislation on data protection which is also expected to be the case in other developing countries. A Kenyan lawyer, Mathew Ngugi observed that, there is lack of analogy between most cyber crimes and their conventional counterparts (Ngugi, 2005). He compared trespassing and hacking into a computer network. The penalty on trespass does not hold against hacking and accessing private data. This clearly illustrates a challenging situation whereby no relevant laws on hacking are available.

People in developing countries are widely using the internet. Though convenient, there are few sufficient regulatory mechanisms on data access. Makokoba (2018) cites Zimbabwean government, as not being able to do much to censor the internet. Instead, the government limits access to internet. This significantly illustrates how developing countries want to benefit from new technologies without laying a proper foundation of regulatory procedures on data protection. Froomkin (1996) in his study of internet access in Singapore noted that "information deemed obscene (pornography) in one jurisdiction may be legal elsewhere". This illustrates the conflicting legal provisions of internet regulation for different countries.

Censorship is an important aspect of internet regulation. Governments' legal structures have been challenged in court. For instance, the Zimbabwe government was challenged by private mobile phone providers through a high court order restraining the government from controlling the information gateway system for the providers (Africa.aspx, 2006). This illustrates how data regulatory mechanisms in developing countries are still in want

Unethical Computer Use in the Office or Business Atmosphere

Ethical practices in the work environment form the basis of success for any business venture. Boulton (ud) observed that "employees in small business firms are likely to pirate software, a practice that is seemingly endorsed by the management for purposes of business survival". The main challenge here is piracy within the office/business atmosphere where the superiors may not regulate their users. Otherwise, there may not be clear guidelines on ethical practice in the office. Piracy of data is practiced by experts with the necessary technical knowledge. For example, IT (Information Technology) consultants may use pirated software to complete certain projects. Some firms accept projects that involve software they cannot afford to purchase and seek illegal means of obtaining such software (Boulton, ud). Developing countries experience this problem because of the increasing unemployment trends, where people survive by using illegal business practices to make a living. The use of the internet in the office acts as an entry point to pirated software. Illegal transactions can be carried over a network without being noticed. For example, Froomkin (1996) observed that, trans-border gambling can go on over the internet, evading regulations imposed by jurisdictions in their countries.

Ethical use of computers in the office is challenged by lack of proper guidelines on privacy. Invading a computer to find out what an employee is doing is interfering with his privacy. On the other hand, restricting internet use in the office is different (Weckert, 2000). For example, a survey carried out in three different companies situated in Nairobi, Kenya on employee monitoring, of the employees interviewed, 50% said that they were being monitored secretly when working with the computer, 30% felt that work ethics should guide a person and not monitoring from superiors and 20% felt that monitoring was okay only if it is objectively done. This illustrates the state of affairs in developing countries implying that there are no clear guidelines on privacy and information access at work place. This challenges the employee who should be an agent of privacy at work place. This is why; Bynum (2000) explains that, there are always problems in the application of computer ethics because there are no clear policies of how computer technologies should be used.

Computer System Mal-Function And Hardware Failure

Data should not only be protected from people (users) but also from computer systems that either not functioning well or hardware that fails to function appropriately. System operations are related to the software used. System failure, according to Meadowcroft (2005), may result from the complexity of the software used. Developing countries are using modern software which is more complex and efficient in operation. If there is improper coding of software, the system is likely to fail. Data held in such a system is also likely to vanish if the system malfunctions. System failure can result from the user e.g. when the user gives the computer inaccurate instructions. This may lead to loss of files and indeed data held in these files (Capron, 1996).

Certain types of hardware such as diskettes are vulnerable to conditions such as extreme temperatures, scratching, pressure and presence of magnetic fields (Capron, 1996). As such, data in them is likely to be lost because of such conditions. This is common in developing countries because the hardware being sold to consumers is of low quality and quite susceptible to the said conditions.

Identity Theft and Credit Card Theft

Cameron (2018), noted that “data reveals the global circulation of stolen identities is leading to major shifts in cybercrime worldwide, with developing countries cultivating newly formed internet-based economies responsible for a generous amount of fake and stolen account activity”. Notably, as e-commerce markets in Latin America continue to expand, incidents of fraud are beginning to skyrocket. Stolen and forged identities used to create fake accounts is, in turn, becoming a market unto itself. It has to be noted that billions of online users are generating huge amounts of personal data and this makes it easier for cybercriminals to steal and monetise this. Data which has been stolen gives cybercrime a deceptive mask, as they take over identities to open new accounts, takeover legitimate user accounts or perform fraudulent transactions.

Cameron (2018), noted that “in the first quarter of 2018, researchers registered more than 150 million rejected transaction, indicating online fraud is soaring; the figure represents an 88 percent increase from the same period in 2017”. Moreover, new and emerging economies Egypt, South Korea, Ecuador, Ukraine, and Vietnam, are offered as examples, have contributed to 820 million bot-based attacks targeting ecommerce sites worldwide (Cameron, 2018).

The challenges having been looked at, the chapter will continue to look at the arguments for and arguments against internet privacy.

REMEDIES TO THE CHALLENGES

Internet Regulations for Both Users and Internet Service Providers

New technologies contribute to the national development of developing countries. However, challenges due to the technological advancement retard the growth of some sectors of the economy. Internet access is one of the main issues. Developing countries need to initiate self regulation mechanisms. Bullesbach (2004) observed that “adequate data protection is effective when countries initiate data protection by means of self regulation”. This is an important aspect for developing countries because of the different cultural diversities of their people. Self regulation mechanisms would cater for all diverse cultures different from the western countries. Palfrey (2005) observed that “internet service providers must be encouraged to establish codes of conduct that prohibit their users from using the internet to access illegal information or doing illegal business transactions”.

Developing countries should embrace a self regulatory approach by encouraging their internet service providers to regulate their customers by establishing regulatory mechanisms internal to their businesses. This would cultivate ethics among customers in using the internet. Spamming can also be controlled by using combined efforts between law enforcement agencies and internet service providers. Instead of chasing spammers, according to Palfrey (2005), regulators in less developed countries can only succeed by working in liaison with internet service providers who are closer to the source of the problem i.e. their customers and the technology in question. Due to the complexity of spamming, developing countries can avail resources and the necessary personnel to help combat spamming.

The primary role of data access and protection lies with the users. The users must be ethical in accessing data. Unethical users need to be legally regulated. This is why; Barroso (2001) cited that “internet use should be legally regulated besides having the users’ role in its regulation”.

Computer Ethics Education and Training Among Users

Ethical practices are an important component of any professional field. In this era of Information and communication technology, a lot of data relating to people, governments and business organisations is being handled by computing professionals. As a result a high level of ethical practice is essential. Ethical practices can be imparted to computing professionals during their course of study or being given in-service training. Weckert (2000) noted that “there must be involvement in the education of computing professionals”.

Ethical practices in developing countries should serve a central role in alleviating data crimes. Computer users in these countries should be trained on ethical issues related to data protection. There is a need for refresher courses on emerging issues such as internet pornography, spamming, hacking and other forms of cyber crime. All these issues are as result of the advancement in information and communication technology. The main remedy is therefore a code of practice for all computing professionals and service providers in information and communication technology. Not all computer-related infringements are noticed. This is why all computing professionals should regulate their practices in an ethical point of view. As Barroso (2001) noted “the cyber society in which we live needs an ethics of the internet and that internet ethics depend on the receiver or navigator”. As a result, internet service regulatory bodies and internet service providers can educate their customers about certain dangers of internet communication (Palfrey, 2005).

Personal data should also be protected from unauthorised access. A culture of personal data protection should be cultivated among users. Lace (2005) proposed that “people should be made aware of how to protect their personal data and resist any mal-practices involving their data”. The integrity of data depends on the end user. For instance, if a user is well trained, the chances of the system failing are greatly reduced which improves the reliability and integrity of data (Meadowcroft, 2005).

Computer ethics education requires a global approach for harmonisation. All stakeholders must be involved if meaningful solutions to computer ethics are to be provided. Weckert (2000) proposed that “a number of disciplines must cooperate so that meaningful answers to computer ethics are to be provided”. Employers must cooperate with their employees on matters of computer ethics. Cheung (2000) observed that “the induction of new employees to the culture is a central measure of data protection”. Since different organisations may deal with data differently, new employees need to be introduced to all aspects of data protection.

Cross-Border Harmonisation of Laws on Data Protection and Enforcement Procedures

Data protection requires concerted efforts which must involve harmonisation of new or existing legislation. These laws must have an international setting and applicable to all states regardless of whether a country is developed or not. Conflicting or no laws at all hampers the fight against illegal data access and cyber crimes. Developing countries need to establish common laws that can be uniformly applied in different countries for the same crime. Ngugi (2005) proposed that “there is a need to act in concert with the global community in combating cyber crime”. He further observed that, legislations on data protection should provide for dual criminality in case a culprit crosses borders (Ngugi, 2005). Relevant stakeholders in developing countries should therefore hold common forums within which certain laws can be harmonised. Harmonisation implies cooperation between different countries. Bullesbach (2004) noted that “international harmonisation of principles of data protection ensures international data transfers in global markets”. This implies that illegal data access will be minimised by use of common principles.

Cooperation could be evident when different countries’ law enforcement agents cooperate in fighting cyber crime. For example, the likes of Interpol. As Brenner (2001) observed, Interpol pursues cyber crime through regional working parties. Palfrey (2005) proposed that, harmonisation and collaboration are essential in fighting cyber crime. This could be an effective method of fighting cyber crime as it illustrates uniformity in law enforcement for different states. Conventions on internet crimes can also aid in fighting cyber crimes. For instance, the United States joined the Council of Europe Convention on Cyber crime on September 29th 2006 (McCormack, 2006). Developing countries should emulate the developed countries by joining such conventions. Froomkin (1996) observed that, without cooperation between the two governments involved, there may be very little the affected government can do to fight the crime. The same idea is applauded by Franco (2006), when he explains that, task forces on minimising piracy have helped stem out such crimes across the borders of Brazil, Paraguay and Uruguay.

Response to System Failure, Hardware Failure, and Power Blackouts

Data needs to be protected against physical factors such as system failure, hardware failure and power blackouts. System failure may depend on the users and this is why users have a central role to play to avoid system failure. The best practices for avoiding system failure, according to Phillips (2004), include user manuals that provide system specifications and also testing the code earlier in advance. Testing of

code is an ethical aspect of software development which affects the system functionality. Meadowcroft (2005) observed that “system testing is important in being prepared for potential system failures”. Developing countries should adopt an ethical culture of using sufficiently tested codes. This would improve data security. Users should also be trained on how to use particular computer system to avoid failure.

Faulty hardware can lead to data loss. To avoid hardware failure, essential functions could be transferred to backup components (Meadowcroft, 2005). Some types of software are also important in backup. Capron (1996) observed that “the use of software that automatically backs up all files is essential for data protection”. Power losses or power blackouts can lead to loss of data. Reliable power sources should be sought.

National Youth Development Forums and Self Employment Initiatives

Developing countries should view youth unemployment as the major source of the numerous economic crimes including data piracy. The youth should play an important role in data protection. Governments in developing countries should initiate forums that are aimed at educating the youth on self employment and also organising workshops for educated but unemployed youth. They should establish youth groups whose main objective is to eradicate data crimes. Such forums can be used to disseminate ideas on cyber crimes and the role of the youth in alleviating such cyber crimes.

Arguments for Internet Privacy Concerns

Consumers are really interested in the safeguard of their privacy. Surveys show that the primary reason most non-Internet users avoid the Internet is because of the concern about the privacy and safety of their personal information and communications (Federal Trade Commission, 1998). Privacy concerns prevent some consumers from buying products on the web. A marketing research firm, NFO Interactive, conducted a study in 1999 and found that almost three out of four consumers who browse the Internet never make any purchases online (James, 2000). Those consumers said that they would be more likely to buy if they could be assured that their privacy would be respected (James, 2000). A study by Satitkit (2001), on the travel sector in New Zealand suggested that “privacy and security were the concerns that stopped people from purchasing travel tickets online”.

Although personal information may not be used after collection, it must be noticed that collecting and keeping this information is a potential liability for a web site when it meets some consumers that take the safeguard of their privacy seriously. Internet based businesses should care about the privacy concerns because consumers care about it. Since businesses are developing relationships with consumers, it helps if consumers know that businesses care about them. People are more comfortable if they see a privacy statement, and are more assured if a privacy statement has been approved by a third party, such as TrustE [10, 24] (Satitkit, 2001). To boost the development of e-commerce, information privacy concerns should be treated seriously as these discourage consumers from using the Internet in buying goods and services (Federal Trade Commission, 1998).

Arguments Against Internet Privacy Concerns

To some people, Internet privacy concerns are not special issues, and some are just over sensitive as they realise that the Internet is growing. Shopping online is not different from in-store shopping as these both raise the same privacy concerns. Tracking a person’s navigation while online can be compared to

a camera spying on people while they are moving around in a store. Although cookies can be used to identify users to a web site, cannot find out names, addresses, and other personal information unless consumers have provided such information voluntarily (Cattapan, 2000). Thus, the use of cookies is not a main point regarding the privacy concerns. The Roy Morgan Research (2001) in its findings noted that “it is a fact that some people are willing to give away their personal information in return for discounts and other particular benefits. An example is the befoward platform for purchasing vehicles whereby one creates an account with personal information so as to get discounts as well as online news and alerts. The use of cookies for online purchases is not different from catalogue purchases by mail when personal information is provided voluntarily. They both raise the same privacy concerns that information may be misused when it gets to the hand of the businesses.

Another argument emphasises that Internet privacy concerns are trivial. Consumers do not want to reveal their information online for marketing purposes. Actually consumer information can also be found in telephone books or other sources. This information can usually be used by marketers for marketing promotions. Marketers can send flyers to physical letterboxes based on this information. It is argued that getting rid of junk email is easier than getting rid of junk physical mail. Thus, the privacy concerns regarding junk email are considered to be trivial.

Use of internet Regionally and Internationally

In a study by Ericsson Consumer Lab (2014), the growing adoption of smart phones in Southern Africa significantly increased Internet access within the local populations. The research study showed that “approximately 70% of Internet users in sub-Saharan Africa access the Internet through their mobile phones compared to 2% who use computers”. Access to social network sites such as blogs, YouTube, Twitter, Instagram, LinkedIn, and Facebook has also increased significantly. According to the Internet World statistics (2018) as of 31 December 2017, Estimated Internet utilisation in Zimbabwe was at 35, 2% while the rest of the world was at 58,4%. Internet users in Zimbabwe were estimated at 50 000 in 2000, while in 2017, estimated users were at 6 796 314. Compared to the Americas, Internet utilisation was at 100% with a total of 783 909 293 estimated people. This increase in Internet penetration and usage also increases concerns about online privacy. In developed countries such as USA, many studies have been conducted to assess Internet users concerns about privacy, but little is known for the Southern African countries.

Personal Data Protection Legislation

Deloitte (2017) notes that “many Internet users express demand for legislation that protects their privacy online”. Moreover, there are currently 17 countries in Africa that have enacted comprehensive personal data protection legislation, namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara¹. In addition, the African Union (AU), adopted the AU Convention on Cybersecurity and Data Protection (AU Convention) in June 2014 (Rich, 2016). However, the AU Convention has not currently taken effect as it has, to date, not been ratified by 15 out of the 54 AU member jurisdictions (Rich, 2016). Nonetheless, the AU Convention does provide a personal data protection framework which African countries may potentially transpose into their national legislation, and encourages African countries to recognise the need for protecting personal data and promoting the free flow of such personal data, taking global digitalisation and trade into account. In this regard, Rich (2016) notes that “there

are three countries, namely Kenya, Uganda and Zimbabwe, which have already enacted personal data protection legislation, the promulgation of which has not yet been made effective, as the laws are still in the form of bills”. Tanzania is another country which is currently in the process of enacting personal data protection legislation (Rich, 2016).

An early study on general online privacy awareness and concerns was done by AT&T in 1998 (Cranor et al, 1999), with the aim of understanding how American user are concerned with their online privacy. The sample was drawn from the FamilyPC magazine/Digital Research, Inc. Family Panel to represent the future Internet population of the USA. The finding indicated that 52% of Internet users were concerned about web cookies, and among those concerned, 56% had taken measures to change their cookie settings to something other than accepting all cookies without warning (Cranor et al, 1999).

A more recent study on user concerns on Anonymity, Privacy, and Security Online was done by the Pew Research Center in 2013 (Ruhwanya, 2015). This study was directed to American Internet users and data was collected from telephone interviews among a sample of 1,002 adults. The study shows a growing level of privacy concern for Internet users, in practice, “86% of Internet users have taken steps online to remove or mask their digital footprints – ranging from clearing cookies to encrypting their e-mail, from avoiding using their name to using virtual networks that mask their Internet protocol (IP) address ” (Ruhwanya, 2015).

SOLUTIONS AND RECOMMENDATIONS

Most Internet users spread their own personal information and sign privacy policies without even giving it a second thought. This behaviour verifies the fact that people are oblivious about their own privacy. However, blame cannot be put on the end user, corporations must take responsibility when they formulate privacy policies so that the users understand the content of them and in particular explain how what they do with the information. Email is one of the most important and applied features on the Internet but the unrestrained growth of spam threaten its functionality. A solution to this requires cooperation between online actors, legislatives and educators. Overallly, there is a need for cooperative legislatives amongst countries within the five continents of the World. This will allow for uniformity.

FUTURE RESEARCH DIRECTIONS

A number of further questions arose during the study. It would be useful to conduct research for each developing country separately and take on a random national sample of the Internet users; study why some personal data are more sensitive in developing than to developed and vice versa; and study further why developed countries are more aware of measure to conceal online privacy than developing countries. This information would benefit Communication Regulatory Authorities in developing countries, who could adopt to the approaches and findings reported in this chapter to better understand their consumers’ behaviour regarding internet privacy and see how they can regulate the privacy policies to align with user needs.

CONCLUSION

The majority of the legal protections are laws that were enacted long before the Internet was commercially available and were just applied to the Internet as if it were any other technology. With no federal law protecting privacy on a universal level for adults, there is room for improvement. The burden of protecting online privacy has fallen to the user who is expected to read an obscene amount of text found in terms of use agreements and determine how to respond if they do not agree with the terms presented to them. If they do not agree, but have no choice but to sign or didn't read the terms until after they already signed the agreement they are left to using technological means to protecting their privacy. Overall, situation in regards to protecting online privacy in the United States is depressing. While there is most certainly room for improvement, it may take over a decade before any true progress is made. Until then, the best hope for privacy is that the technological protections outpace the threats to online privacy.

REFERENCES

- Access to Information and Privacy Act (Zimbabwe). (2002).
- Africa.aspx. (2006). Zimbabwe: Econet and Telecel seek court order to block new regulation. *The Herald*. Retrieved December 11, 2018, from <http://www1.herald.co.zw/inside.aspx?sectid=11033&cat=1&livedate11/6/2006>
- Anstead, M. (2000). *Taking a tough line on privacy*. Marketing.
- Banistar, D. (2006). *Freedom of information around the World*. Retrieved 18 March 2017, from http://www.humanrightsinitiative.org/propagrams/ai/international/laws_paper/intl/gobal_foi_surbey_2006.pdf
- Barroso, P. (2001) Cyberspace: Ethical problems with new technology. *Ethicomp*.
- Brenner, S. (2001). *International law enforcement*. Retrieved October 21, 2018, from <http://www.cybercrimes.net/International/LawEnforcement.html>
- Bullesbach, A. (2004). *Current challenges of data protection in the world economy*. Retrieved, September 30, 2018, from http://www.26konferencja.giido.gov.pl/data/resources/BullesbachA_pres_en.pdf
- Bynum, T. W. (2000). *A very short history of Computer ethics*. Retrieved from http://www.southernct.edu/organizations/rccs/textonly/resources_t/research_t/introduction_t/bynum_shrt_hist_t.html
- Cameron, D. (2018). Privacy and Security. Identity theft is exploding in the developing countries. *Cybercrime*. Retrieved September 9, 2019, from, <https://gizmodo.com/identity-theft-is-exploding-in-developing-countries-1825745097>
- Capron, H. L. (Ed.). (1996). *Computers: tools for an information age*. The Benjamin/Cummings Publishing Company, Inc.
- Cattapan, T. (2000). Destroying e-commerce's "cookie monster" image. *Direct Marketing*, 62(12), 20–24.
- Chung, W., & Paynter, J. (2002). Privacy Issues on the Internet. *Proceedings of the 35th Hawaii International Conference on System Sciences*. 10.1109/HICSS.2002.994191

Cranor, L., Joseph, R., & Ackerman, M. (1999). Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. In Telecommunications Policy Research Conference (pp. 25-27). Academic Press.

Cranor, L. F. (2004). I didn't buy it for myself. In Designing personalized user experiences in eCommerce (pp. 57-73). Academic Press.

Deloitte. (2017). *Privacy is paramount: Personal data protection in Africa*. Retrieved October 12, 2018, https://www2.deloitte.com/.../za_Privacy_is_Paramount-Personal_Data_Protection_in_

Ericsson ConsumerLab. (2014) Retrieved October, 11 2018, from, <http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf>

Federal Trade Commission. (1998). *Privacy Online: A Report to Congress*. Retrieved March 3, 2018 from available in <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>

Franco, I. G. (2006). *Striving For Legality*. Retrieved, September, 20, 2018 from <http://www.ipfront.com/depts/articles.asp?id=13202&deptid=6>

Froomkin, A.M. (1996). The internet as a source of regulatory arbitrage. *Asian Examples of Practical Limits to Censorship*.

Internet World Stats. (2018). *World Statistics*. Retrieved October 12, 2018, from <http://www.internet-worldstats.com/stats1.htm>

James, G. (2000). The price of privacy. *Upside.*, 12(4), 182–190.

Kelly, E. (2016). Congress looks to boost email privacy; Increase social media surveillance. *USA Today*. Retrieved September 29, 2018 from, <http://www.usatoday.com/story/news/2016/02/21/congress-looks-boost-email-privacy-increase-social-media-surveillance/80557184/>

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*. Retrieved September 6, 2019 from, <https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527>

Makokoba, W. (2018). *What we know about personal data protection in Zimbabwe*. Retrieved December 12, 2018 from, <https://kalabashmedia.com>

McCormack, S. (2006). *United States joins Council of Europe Convention on Cybercrime*. Retrieved from <http://www.state.gov/r/pa/prs/ps/2006/73353.htm>

Meadowcroft, B. (2005). *System failure: why systems fail*. Retrieved November 2, 2018 from <http://www.benmeadowcroft.com/reports/systemfailure>

Ngugi, M. (2005). *Law on Cyber crime Overdue*. Legal Week, Computer Crime Research Centre. Retrieved, December10, 2018 from <http://www.crime-research.org/news/22.5.2005/982/>

Palfrey, P. (2005). “*Stemming the international tide of spam*”, *A draft model law*. Research Publication.

Paynter, J., & Pearson, M. (1998). An analysis of WWW-based Information Systems. In W. S. Chow (Ed.), *Multimedia Information Systems in Practice* (pp. 53–63). Singapore: Springer.

Pew Research Center. (2013). *Anonymity, Privacy, and Security Online*. Retrieved September, 23 2018, from <http://www.pewinternet.org/>

Phillips, D. (2004). *“Elements of effective software management”, the project managers hand book*. IEEE Computer Society Press. doi:10.1109/9780471677772

Piirsalu, K.-L., Mäe, D., Vassar, T., & Nani, A. (2012). *Privacy issues of Social Networks*. Retrieved September 10, 2016, from, <http://social-networks-privacy.wikidot.com/>

Rambam, S. (2010). *Privacy Is Dead – Get Over It at The Next HOPE, July 16-18, 2010 in New York City*. Retrieved February 8, 2018, from https://www.youtube.com/watch?v=DaYn_PkrfvQ

Rich, C. (2016) *Privacy Laws in Africa and the Near East*. Bloomberg BNA World Data Protection Report.

Risen, T. (2015). The illusion of online privacy. *The US News & World Report*. Retrieved October, 3 2018, from <http://www.usnews.com/news/articles/2015/08/25/the-illusion-of-online-privacy>

Rosner, G., & Kenneally, K. (2017). *Privacy and the Internet of Things: Emerging Frameworks For Policy And Design*. Center For Long-Term Cybersecurity. Retrieved September 5, 2019, from, https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf

Roy Morgan Research. (2001). *Privacy and the Community, July 2001*. Office of the Federal Privacy Commissioner. Retrieved September, 4 2018, from, <http://www.privacy.gov.au/publications/rcommunity.html>

Satitkit, S. (2001). User Perceptions of Web site Design in the Travel Industry: an Evaluation Model (Unpublished MCom project). University of Auckland.

Sidbury, B. F. (2001). You’ve got mail...and your boss knows it: Rethinking the scope of the electronic communications privacy act. *Journal of Internet Law*, 1(5), pp16–pp22.

Stefanie, O. (2001). Reversal of fortune – tracking web trackers. *ZD Net News*. Retrieved October 6 2018, from <http://www.zdnet.com/zdnn/stories/news/0,4586,2692472,00.html>

The Editorial Board. (2017). Republicans Attack Internet Privacy. *New York Times*. Retrieved March 29, 2017 from, <https://www.nytimes.com/2017/03/29/opinion/republicans-attack-interest-privacy.html>

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4), 451–470. doi:10.1080/08838151.2012.732140

Weckert, J. (2000). *Computer ethics: future directions*. Retrieved November 13, 2018, from <http://www.acs.org.au/act/events/2000acs4.html>

Wheeler, T. (2017). How the Republicans Sold Your Privacy to Internet Providers. *New York Times*. Retrieved March 29, 2017 from <https://www.nytimes.com/2017/03/29/how-the-republicans-sold-your-privacy-to-internet-providers.html>

Wiki/computer crime. (2006). *Computer crime*. Retrieved December 3, 2018, from http://en.wikipedia.org/wiki/computer_crime

Yanisky-Ravid, S. (2014). To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory. *American University Law Review*, 5(64), 53-108. Retrieved September 19, 2018 from <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1939&context=aulr>

ADDITIONAL READING

Deloitte. (2017). Privacy is paramount: Personal data protection in Africa. Retrieved October 12, 2018, https://www2.deloitte.com/.../za_Privacy_is_Paramount-Personal_Data_Protection_in_

Palfrey, P. (2005). “*Stemming the international tide of spam*”, *A draft model law*. Research Publication.

Sidbury, B. F. (2001). You’ve got mail...and your boss knows it: Rethinking the scope of the electronic communications privacy act. *Journal of Internet Law*, 1(5), pp16–pp22.

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4), 451–470. doi:10.1080/08838151.2012.732140

KEY TERMS AND DEFINITIONS

Developed Country: A self-governing country with advanced technological infrastructure, a developed economy as well as an advanced industry.

Developing Country: A country that is still seeking to become advanced in all spheres that is industrially, economically, politically, and socially.

Internet Privacy: This is the privacy and level of personal data and or information published online (via the internet).

Internet Utilisation: The amount of data flowing through a computer or device (mobile phone, tablet) for a given period of time.

Privacy Protection: The coexistence of the collection and dissemination of information communication technologies, what the public expects as well as socio-political and legal concerns bounding them.

Privacy and Security Challenges in the Internet of Things

Fernando Almeida

 <https://orcid.org/0000-0002-6758-4843>

Polytechnic Institute of Gaya, Portugal

Justino Lourenço

Polytechnic Institute of Gaya, Portugal

INTRODUCTION

The Internet of Things (IoT) is a concept that describes the large and growing number of digital devices that operate between networks of potentially global scale. Unlike the conventional Internet, in which interaction is essentially performed by people, IoT is composed only of sensors and other intelligent devices (Chou, 2016). Therefore, we are facing a technological revolution that includes the interaction between objects and simple actions of daily life to the most complex processes of organizing entire industrial productions. IoT provides new and innovative ways for organizations to manage and monitor remote operations (Vermesan & Friess, 2014). Conceptually, it offers the possibility of connecting the physical world with the digital world through the Internet.

Significant social and material vulnerabilities can appear with the advancement of IoT. The Internet exposes people to new risk situations, which although they already exist in the physical world, are enhanced in the virtual world, due to the greater exposure and range that technologies provide. Several risks may arise due to IoT's lack of privacy and security. For example, hackers can open the door of a house remotely by knowing access security codes, can know user behaviors through access to the network of home light sensors or temperature sensors, can spy a person through access to security cameras, etc. (Eastwood, 2017; Karlov, 2017). Therefore, it is critical that IoT provides strong security mechanisms in a way that the benefits of this technology could be safely exploited by people.

The large network of connected devices and the enormous flow of data that IoT will generate turn data security and privacy a fundamental challenge. In this sense, this study aims to characterize how IoT service providers address the challenge of data privacy and security. By conducting case studies with leading companies in this sector we seek: (i) to identify the main privacy risks that IoT devices can expose; (ii) analyze the main privacy and security barriers in IoT devices; and (iii) propose counter-measures that can be adopted by companies and users to increase the security of IoT. The manuscript is organized as follows: initially a literature review on the concept of IoT and security and data protection is performed. After that, the adopted methodology is presented. Consequently, the main identified solutions and recommendations are presented and discussed. After that, some indications for future research are given. Finally, the main conclusions are drawn.

DOI: 10.4018/978-1-5225-9715-5.ch051

BACKGROUND

Concept, Evolution and Technologies of IoT

IoT is a concept in which the devices and objects of our day-to-day life are equipped with sensors capable of intelligently communicating between them. According to Hanes et al. (2017) a “thing” in the context of the IoT is a connected object which may be, for example, a person with a heart monitor, an industrial tank with level sensors, a car with sensors that warn of tire pressure, a public lighting of a city, an outlet at home, or any other natural or man-made object. IoT collects information from various devices (computers, vehicles, smartphones, traffic lights, etc.) and applications (anything from a social media application like Twitter to an e-commerce platform, from a production system to a traffic control).

IoT has the potentiality to transform the way we live, work and learn. It is the beginning of a cycle of technological renewal that will aid in the optimization and automation of basic daily tasks. In addition, it may bring important information for the public benefit, and for private companies to be more assertive in their products and services rendered. The virtual connection of data, people, processes and things promises to create a world of new economic opportunities, including Smart Cities, Smart Environment, Smart Metering, Security & Emergencies, Retail, Logistics, Industrial Control, Smart Agriculture, Smart Animal Farming, home automation and e-Health (Talari et al., 2017). For Kash (2014), some practical examples of IoT application are:

- Intelligent parking systems for cities will provide real-time visibility into the availability of parking spaces throughout the city;
- Teleworking can eliminate the daily path of the workplace, allowing employees to work from home. In remote locations, it would reduce costs and improve productivity for employers and employees. The impacts would result in reduced employee spending, office maintenance and cleaning, increased employee retention, increased productivity and new job opportunities;
- Intelligent transportation solutions improve traffic flows and reduce fuel consumption;
- Intelligent power grids more efficiently connect renewable resources, improve system reliability, and consumers are charged based on the efficiency of the operation;
- Through intelligent medicine, doctors and hospitals can receive and organize data from connected medical devices, including wearable and health monitors installed in patients' homes. By receiving the data in real-time, medical professionals thus obtain more complete information of their patients, improving care through more effective diagnoses and treatments;
- Machine monitoring sensors diagnose and anticipate pending maintenance problems and lack of stock.

IoT encompass every aspect of our daily lives, because it literally enables billions of things to be connected anytime, anywhere, to anything or any person. Its applications are many, such as smart houses, connected cars, energy systems, agriculture, transport, health, etc. A single technology cannot effectively meet all the needs of IoT's many applications. Therefore, although some objects use wired connections like Ethernet, Wireless communication technologies play a crucial role in enabling IoT connectivity. According to Kranz (2016), an ideal IoT communication network will be a mixture between the two types, Wired and Wireless. Several technologies can be used in IoT, respectively:

- Wi-Fi – a wireless local area network (WLAN) that transmits via standard IEEE 802.11 radio waves, with a maximum range of 50 meters and a connection speed of 2.4GHz or 5GHz ultra-frequency. This technology is appropriate for transferring large amounts of data between devices. However, this requires a lot of power to operate, while many IoT devices require a much lower data transfer rate than that used by Wi-Fi. This means the batteries of the devices have to be changed on a regular basis;
- Bluetooth – suitable for short-range communications. It transmits data at a bandwidth between 2.4 and 2.485GHz. It operates at distances shorter than Wi-Fi and requires less power to operate. Smart Bluetooth is an important protocol for IoT, because it offers a range similar to Bluetooth but designed for significantly reduced power consumption. However, Smart Bluetooth is not really designed for file transfer and is best suited for small blocks of data;
- Zigbee – enables devices with low operating power, low data rate and low cost of implementation to send data on the network, with each device capable of retransmitting the data towards its intended destination. Its main virtue is its low price and low power consumption;
- Z-Wave – technology, primarily designed for home automation (e.g., products such lamps, sensors, among others). Optimized for reliable, low-latency communication of small data packets with transfer rates between 100kbit / s, it operates in the sub-1GHz band, not interfering with 2.4GHz bandwidth, such as Bluetooth or Z-Wave;
- RFID – technologies that use the radio frequency for data capture. There are several methods of identification, and the most used is to store a serial number that identifies the information in a microchip. Such technology allows automatic capture of data, for identification of objects with electronic devices, known as electronic tags, tags or RF tags, which emit radiofrequency signals to readers who collect this information. This technology can have several applications, such as: security and access control, traffic control of vehicles, personal identification, animal screening, identification of objects, etc;
- NFC – technology that allows data transfer in short distance wireless communication. The NFC has emerged from RFID and, consequently, many of the benefits observed in the previous point are shared by both technologies. Like in RFID, the communication is done in a simple and intuitive way, just by bringing two devices together, or the device and a passive tag, at a short distance. The speed of the NFC throughput is 424 kbits and operates at the frequency of 13.56 MHz.

The existence of a large number of different technologies makes the role of standards more relevant since they provide a way of solving a problem by ensuring the compatibility between different devices. Open standards perform a crucial role in enabling interoperability (Almeida et al., 2010). IoT involves the connection between devices that in most cases were never thought to be connected. It also involves managing those devices and developing applications to do things together that they would never do alone. Consequently, IoT service providers have been advancing with the development of standards by creating alliances for this purpose. These efforts (e.g., AllSeen, Open Interconnect Consortium, Industrial Internet Consortium, etc.) have been developed in key areas of IoT, such as connectivity, interoperability, privacy and security (Naito, 2017; Sethi & Sarangi, 2017).

Security and Data Protection

One of the most demanding challenges for IoT is how data security and the consumers themselves will be guaranteed. Like it happens with smart metering equipment and increasingly autonomous cars, there will be a vast amount of data providing information on the personal use of devices that, if unsafe, could pave the way for privacy breaches. According to Qin et al. (2016), this is a challenge because the high volume of information generated by IoT is essential to bring better services and communities to consumers. Additionally, trust is a key element in the adoption of IoT services. AlHogail (2018) states that it is vital that consumers interact with interconnected IoT devices and systems safely, reliably and intuitively.

The IoT environment is commonly formed by a network of devices connected with sensors. These devices are responsible to transmit the gathered information and specific events to a server. This transmission is made through fixed or mobile communication. Privacy should then be protected at the device level, while communicating with the server, on the server data store, and on processing (Maple, 2017; Yang et al., 2017). In the first case, at the device level, sensitive information can be stolen in the case of manipulation of the hardware or software of the device itself. During communication with the server, the most commonly used approach is encryption. Although it is the most widely used, it may not be the safest, since encryption usually stores data in packets that leave traces, like its sequence number, etc. In relation to the privacy in the storage that is done in the server, it must be filtered of, storing the minimum of possible information, or only what the consumer consents (Liu et al., 2017). Finally, the supplier of each device may use the information collected from these same devices for a variety of purposes, including: analysis or marketing. The user must therefore be able to know what use is given to his data, and whether or not to consent to it being used for a purpose other than the initial and consented (Poudel, 2016).

The challenges of privacy and data protection in IoT can be grouped into five dimensions (Ziegeldorf et al., 2014; Zhou et al., 2018):

- Lack of control and asymmetry of information – the interaction between objects that communicate automatically, and between objects and back-end systems will result in the generation of data streams that can hardly be controlled with the traditional tools used to ensure the proper protection of the interests and rights of the data subjects. This issue of lack of control also concerns areas such as cloud computing or big data, and is even more challenging when it is thought that different emerging technologies can be used in combination;
- Perception of user consent – in many cases, the user may not be aware of the processing of data by certain devices. The possibility of rejecting certain services is not a viable alternative in IoT, and the classic mechanisms used to obtain consent are difficult to apply. Therefore, new ways of obtaining user consent for connected devices should be considered by their manufacturers;
- Redefinition of original data processing – the increased amount of data generated by IoT in combination with modern data analysis and cross-matching techniques may give rise to secondary uses of the same data, whether or not related to the processing purpose initially assigned to the devices;
- Identification of patterns and relationships – although each device generates data streams in isolation, its collection and subsequent analysis can easily reveal individual patterns, behavior, preferences and habits;
- Limitations of user anonymity – the full development of IoT's capabilities can put pressure on the current possibilities of anonymous use of services and limit the possibility of uses to remaining anonymous.

FOCUS OF THE ARTICLE

The article has three main goals: (i) identify the main privacy risks that IoT devices can expose; (ii) analyze the main privacy and security barriers in IoT devices; and (iii) propose countermeasures that can be adopted by companies and users to increase the security of IoT.

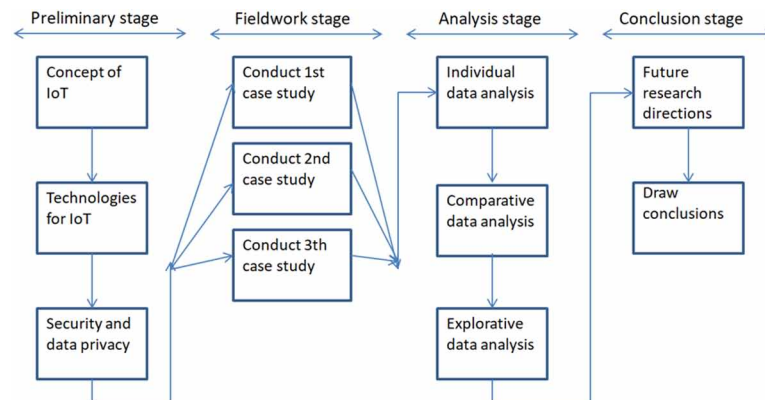
This study uses a qualitative methodology by conducting three case studies with IoT service providers. Qualitative research essentially privileges the understanding of problems from the perspective of research subjects. According to Creswell & Poth (2017), the qualitative approach allows us to describe an in-depth phenomenon through the capture and understanding of individuals' perspectives and points of view on a given subject. The main objective of this approach is not to provide generalizations, but to particularize and understand subjects and phenomena in their complexity and uniqueness (Queirós et al., 2017). In this study, the concrete description of the experiences and representations of the individuals leading to a contextual understanding of the phenomena was preferred in opposition to the universal theory and the explanation of the phenomena in a linear causality.

The case study method has been increasingly used in the social sciences, economics and engineering as a procedure for analyzing reality (Yin, 2017). Stake (2005) and Yin (2017) report case study is a methodological approach that allows the researcher to analyze with intensity and depth several aspects of a phenomenon, a problem, or a real situation. Additionally, Gomm et al. (2014) advocate that case study is an empirical research strategy especially useful for phenomena whose frontier between the phenomenon and context are not absolutely obvious. In this context, the collection of information on the main privacy risks and security barriers with the IoT service providers reveals adequate since it is these companies that better know the reality and the innovation of the sector. Consequently, they are also the ones who can best propose countermeasures that can be adopted by companies and users to increase the security of IoT.

The adopted methodology to conduct this study is depicted in Figure 1. It is composed of four sequential stages: (i) preliminary stage; (ii) fieldwork stage; (iii) analysis stage; and (iv) conclusion stage. In the preliminary stage, the concept of IoT is defined and explored in its multiple dimensions. Next, this study analyzes the communication technologies that allow enhancing the use of IoT in several environments such as smart homes, smart cities or wearables and portables. After that, one of the most troubling challenges of IoT is explored, which is how the security of data and its users can be guaranteed. In the fieldwork stage, case studies are carried out with companies that offer IoT products and services in the international market. Afterwards, the analysis stage emerges, which is a crucial point in the methodology. In this phase an individual analysis of the results of each interview is carried out, followed by a comparative analysis of the case studies using a cross-case syntheses, which intends to identify common and individual privacy risks that IoT devices can expose and also explore its main privacy and security barriers, and finally, the explorative data analysis seeks to identify measures that companies and users can implement to increase the security of IoT. Finally, future research directions are discussed, and the main conclusions of this study are listed.

In the process of designing the case studies as suggested by Hancock & Algozzine (2016) the following validity tests were considered: (i) construct validity; (ii) internal validity; (iii) external validity; and (iv) reliability. For that, multiple sources of evidence with an established chain of events were adopted. Additionally, this study used pattern matching to increase internal validity and a replication logic among the multiple case studies to increase the external validity. It is also relevant to emphasize the adoption of a case study protocol proposed by Yin (2017), which composed of five sequential phases:

Figure 1 – Phases of the research methodology



1. Case study design – involved three companies that develop IoT solutions for international markets. Semi-structured interviews were considered and organized into three dimensions as presented in Table 1;
2. Data collection preparation – semi-structured interviews were conducted within these companies. According to Jamshed (2014), semi-structured interviews allow respondents to express freely their point of view and simultaneously encourage two-way communication with the interviewer. Additionally, they provide a reliable method for analyzing comparatively qualitative data (Leung, 2015). The interviews were carried out with the technical managers for the development of IoT solutions in the facilities of these companies;
3. Collecting evidence – informal notes according to each response given by the interviewee were collected by the interviewer. Finally, a preliminary draft of the case study report was created and validated by the respondents;
4. Analyzing evidence – theoretical propositions were used to compare collected evidence on the case studies versus the information collected in the background of this study. Furthermore, cross-case syntheses were adopted to identity common evidences among case studies;
5. Reporting case studies – a final report gathering all the information collected from case studies was compiled.

The profile of the companies selected for the case studies is depicted in Table 2. Although all three companies work in the IoT field, the area of intervention is quite distinct due essentially to the wide range of available technologies and very diverse applications field of IoT, such as games, virtual reality, cultural events, health, smart homes, smart cities, wearables or smart retail.

SOLUTIONS AND RECOMMENDATIONS

Contextual

All interviewed companies are focused in providing end-to-end solutions, offering the best usability and suitability to business needs. They typically develop and integrate Web, mobile and interactive interfaces always with the aim of delivering concrete information, with little or no user interaction. IoT is

Table 1. Interview questions

Dimension	Questions
Contextual	Q1. What is the main business field of your company? Is it only dedicated for developing IoT solutions?
	Q2. What were the main challenges faced by IoT companies during the past years?
Diagnostic	Q3. What are the main technologies adopted in the development of IoT solutions?
	Q4. What are the main privacy risks that IoT devices can expose?
	Q5. What are the main privacy and security barriers to the adoption of IoT solutions?
Strategic	Q6. What are the main countermeasures that companies and users can adopt to increase the security of IoT?
	Q7. What differentiate your companies from your main competitors?

Table 2. Profile of companies

iD	Established date	Description
CS1	2008	Company that develops creative, customized and interactive software for Events, Brand Activators and Museums, Holograms, Virtual Reality, Video-mapping, 4D Rooms, 360° Immersive Rooms, Augmented Reality and Interactive Games.
CS2	2012	National and international consulting company in the telecommunications field. Responsible for the conception, development, implementation and management of national and international technological projects. The company also offers training in the telecommunications field.
CS3	2006	Company that provides engineering solutions with integrated intervention in fixed and mobile networks, new generation networks, systems and all types of technological infrastructures.

one of the actions areas of those companies, as many customers depend on enterprise systems that need rich, near real-time, accurate data, as well as optimized process management. However, IoT is usually a component in an IT wider infrastructure.

Changing the human mentality emerges as the main challenge faced by IoT companies during the past years. CS2 refers that at this level in a first phase the company experienced difficulties due to the lack of knowledge on the part of customers about IoT and, in a second phase, it was consequently necessary to evangelize the end users as well. Other challenges more related to technological issues emerge, such as:

- Integration – a very high number of connected devices makes the integration and concurrent data exchange complex. Additionally, IoT sensors use new and novel communication protocols, which turn difficult to integrate with older devices;
- Security – small devices typically have limited CPU power. Consequently, there is little processing power for implementing security mechanisms. Furthermore, it is important to note that IoT needs to offer mechanisms for identity management and encryption key management;
- Privacy – IoT devices generate a vast amount of critical data that creates potential manipulation risks, for example in terms of identity theft, data falsification, external network manipulation or cybercrime;
- Connectivity – it becomes difficult to ensure that all IoT devices and the system is up and running. Additionally, sometimes data reading can be incorrect due to hardware, atmospheric or environmental issues.

Diagnostic

One of IoT's greatest challenges is the integration of a large number of very diverse technologies. Technologies in this area include the network for Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN), such as RFID, NFC, Bluetooth, Zigbee, WiFi, Winmax or 3G/4G. Other technologies are also typically included in the development of end-to-end applications, such as Java, Python, nodeJS, REST, Elastic Search (ELK), Docker¹ or Kubernetes².

IoT devices operate in hostile environments and a potential attack surface in IoT platforms is much larger than in other traditional systems. Therefore, it requires end-to-end security, from sensors and actuators to management interfaces. Moreover, protocols like Message Queuing Telemetry Transport (MQTT) were not designed with security in mind. Security is often implemented adding a TLS layer, but that's not acceptable for lower end CPU devices without dedicated encryption engines. Consequently, potential privacy risks are spread: sensor data sniffing is a risk, but attacks on backend or analytics subsystems can represent the highest risk, as they can expose the most important and secret business related information. Other potential risk referred by CS3 is that weak configurations tend to persist along the time which creates potential hidden risks that can be exploited in a cyber attack. In this sense, IoT security must be essentially preventive and not corrective. This is particularly relevant in high sensitive industries like healthcare, where the primary goal is to ensure that security network is resilient to prevent data leaks from malicious attacks (Razzaq et al., 2017).

Sense of insecurity can be seen as the main privacy and security barrier to the adoption of IoT solutions. In fact, as mentioned by CS1 the first generation platforms were insecure by design, and that led to improper situations. These notices were quickly shared by several users on newspapers and social networks, which generated a feeling of insecurity that is difficult to combat. Additionally, users may not want there to be an increase in information that is shared. It is therefore essential that there is a right balanced between the desire for new services that make life easier for people and companies, but in which critical and personal data are properly secured.

Strategic

There are good practices and countermeasures that companies and users can adopt to increase the security of IoT. Firstly, it shouldn't be used in production environments anything that wasn't carefully analyzed previously. It is fundamental to consider that security audit tools are essential in any IT infrastructure, but IoT systems require additional deep data traffic analysis, in order to identify improper data streams. CS1 recommends not using arbitrary libraries if the IoT solution is developed internally. Other identified good practice referred by CS3 is the adoption of a risk-driven approach. The idea is to create a risk matrix to all IoT devices and then apply security controls mechanisms suitable to the level of risk involved. The same company also states the importance to automate security when possible. This approach will contribute to have a better data monitoring process.

The differentiation of companies operating in IoT is made based on the creation of integrated solutions. Because the scope of IoT is very broad, there is a wide range of differentiation opportunities. Companies should explore the integration of IoT and other enterprise systems, like Business Process Management (BPM), production management, document dematerialization, Geographic Information System (GIS), and mobile platforms to optimize benefits to the customer.

Table 3. Comparative analysis

Question	CS1	CS2	CS3
Q1	- Development of Web and mobile applications - IoT is used in the scope of those projects	- Provide end-to-end solutions - IoT is one of the action areas	- Provides engineering solutions with focus in the IoT segment
Q2	- Lacks of customers' knowledge - Evangelize end-users	- Human mentality, integration and security	- Connectivity, security, privacy, compatibility and Big Data
Q3	- Only integrate solutions	- Considering not only technologies but programming languages and integration products	- There is a wide and high volume of different technologies, such as REST, Python, Java, Angular, or Kubernetes
Q4	- The great risk is due to an increase in the volume of information	- IoT requires end to end security, from sensors and actuators to management interfaces	- IoT handles data that can be used by mining and machine learning algorithms to obtain very sensitive personal information
Q5	- Users may not want there to be an increase in information that is shared	- Sense of insecurity is a barrier, as first generation platforms were unsecure by design, and that led to improper situations - On the technical side, the lack of embedded crypto engines	- Related with privacy and data leaks
Q6	- Identify critical information - Not used arbitrary libraries in internal developed solutions	- Don't use in production environments anything that wasn't carefully analyzed previously - Use security audit tools - Always apply the generic best practices for IT systems	- Adopt a risk-driven approach - Consider the entire IoT ecosystem - Wherever possible, automate security
Q7	- Working with all kinds of technologies	- Don't be focused on the IoT itself, but act to explore the integration of IoT systems	- Create integrated solutions

Comparative Analysis

Finally, a comparative analysis of the outcomes of each of the interviews conducted in each case study was carried out. The information in Table 3 is organized by the established questions, in which CS1, CS2, and CS3 represent each case study. For each case study, the key points and their main differences are highlighted.

FUTURE RESEARCH DIRECTIONS

IoT adoption is already a reality in society, but there is still a lot of resistance, especially in terms of security and privacy. Many companies are not yet properly prepared for the challenges of IoT, since a change in the culture of these organizations is necessary.

Lee et al. (2017) and Liu et al. (2018) synthesize the main research directions into four domains:

- Networking – research is needed into innovative dynamic routing approaches that prioritize content according to its criticality and importance for increasing networking performance. At this level, research projects in virtualization technology, self-configuration, and self-organization networks stand out;
- Standardization – the proliferation of technologies creates difficulties in interoperability between devices. At this level it is necessary to make efforts in IoT standardization and semantic interoperability;
- Energy consumption – due to the small size of IoT devices it is essential to offer efficient battery management mechanisms. Emerging research in the field of micro battery technologies stands out in this respect;
- Security and privacy – it becomes necessary to increase the awareness of the security and privacy offered by IoT in multiple dimensions, such as integrity, non-repudiation, authenticity, confidentiality, privacy and availability. In this sense, research has emerged in the area of security for cloud computing, security for semantic web and crypto engines that could be embedded into IoT devices.

IoT does not exist without artificial intelligence (AI) and, consequently, this is an extremely relevant research topic. Emerging areas of research in this field include machine learning, autonomous and incremental deep learning, and soft artificial intelligence (Song et al., 2018; Milton et al., 2018; Chatterjee, 2018). The AI will necessarily play a key role in obtaining and analyzing results automatically, thus seeking to integrate knowledge from multiple sources using distributed big data models. The security of this process and the privacy in the treatment of this data are one of the most relevant and challenging topics.

Social Internet of Things (SIoT) is other emergent research field. SIoT represents the convergence of the “Internet of Things” and the “Social Networks” worlds (Mendhurwar & Mishra, 2018). SIoT establishes new type of relationships between objects, such as social object relationship, ownership object relationship, and co-location object relationship and co-work object relationship. Future research is needed in terms of securing the SIoT and trustworthiness management. Other relevant topic is the intelligent data process and use the knowledge produced by IoT devices in big data analytics (Ahmed et al., 2017). Research is being developed in data mining, machine learning, predictive analytics and real-time big data.

CONCLUSION

IoT is a new technological paradigm that aims to transform the way we live and work. IoT offers great opportunities to create new custom products and services, but also countless security and privacy challenges. With IoT devices and connected users on the rise, there will also be an enormous amount of data about how each individual uses a given device or application. This information leaves traces of citizens’ everyday behaviors, providing sensitive information that is intended to be private and anonymous.

Several challenges have been felt by IoT companies mainly in the field of human mentality, security, privacy, connectivity and compatibility. The biggest challenge has been to encourage customers to believe in the success of the IoT market and to evangelize end users. It is also worth highlighting the difficulties experienced by companies in working with such a large number of technologies that pose difficulties of interoperability and compatibility.

Companies can implement several countermeasures to increase the security of IoT. The adoption of security tools is essential in a IoT infrastructure. Therefore, companies must apply generic best practices for IT systems, starting from careful user management and security patches installation. Security mechanisms must consider the entire IoT ecosystem and not single devices. The adoption of a risk-driven approach is another relevant strategy that allows companies to apply security controls appropriate to the level of risk involved. This strategy is particularly relevant in complex IoT environments composed by several IoT devices. Finally, it is important to automate security wherever possible. This approach will turn possible to establish preventive security mechanisms that can contribute to increased automation in data monitoring.

REFERENCES

- Ahmed, E., Yaqoob, I., Hashem, I., Khan, I., Ahmed, A., Imran, M., & Vasilakos, A. (2017). The role of big data analytics in Internet of Things. *Computer Networks*, 129, 459–471. doi:10.1016/j.comnet.2017.06.013
- AlHogail, A. (2018). Improving IoT Technology Adoption through Improving Consumer Trust. *Technologies*, 6(3), 1–7. doi:10.3390/technologies6030064
- Almeida, F., Oliveira, J., & Cruz, J. (2010). Open Standards and Open Source: Enabling Interoperability. *International Journal of Software Engineering and Its Applications*, 2(1), 1–11. doi:10.5121/ijsea.2011.2101
- Chatterjee, J. (n.d.). IoT with Big Data Framework using Machine Learning Approach. *International Journal of Machine Learning and Networked Collaborative Engineering*, 2(2), 75–85.
- Chou, T. (2016). *Precision: Principles, Practices and Solutions for the Internet of Things*. Morrisville, NC: Lulu.com.
- Creswell, J., & Poth, C. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, CA: SAGE Publications.
- Eastwood, G. (2017). *5 of the biggest cybersecurity risks surrounding IoT development*. Retrieved 2018, September 17, from <https://www.networkworld.com/article/3204007/internet-of-things/5-of-the-biggest-cybersecurity-risks-surrounding-iot-development.html>
- Gomm, R., Hammersley, M., & Foster, P. (2014). *Case Study Method: Key Issues, Key Texts*. Thousand Oaks, CA: Sage Publications.
- Hancock, D., & Algozzine, B. (2016). *Doing Case Study Research: A Practical Guide for Beginning Researchers*. New York: Teachers College Press.
- Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., & Henry, J. (2017). *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Indianapolis, IN: Cisco Press.
- Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, 5(4), 87–88. doi:10.4103/0976-0105.141942 PMID:25316987
- Karlov, A. (2017). Cybersecurity of Internet of Things – Risks and Opportunities. *Proceedings of the XXVI International Symposium on Nuclear Electronics & Computing*, 182–187.

Kash, W. (2014). *Internet Of Things: 8 Cost-Cutting Ideas For Government*. Retrieved 2018, September 23, from <http://www.informationweek.com/government/leadership/internet-of-things-8-cost-cutting-ideas-for-government/d/d-id/1113459>

Kranz, M. (2016). *Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry*. Hoboken, NJ: Wiley.

Lee, S., Bae, M., & Kim, H. (2017). Future of IoT Networks: A Survey. *Applied Sciences*, 7(10), 1–25. doi:10.3390/app7101072

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, 4(3), 324–327. doi:10.4103/2249-4863.161306 PMID:26288766

Liu, J., Shen, H., Narman, H., Chung, W., & Lin, Z. (2018). A Survey of Mobile Crowdsensing Techniques: A Critical Component for The Internet of Things. *ACM Transactions on Cyber-Physical Systems*, 2(3), 1–26. doi:10.1145/3185504

Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet*, 9(3), 1–28. doi:10.3390/fi9030027

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, 2(2), 155–184. doi:10.1080/23738871.2017.1366536

Mendhurwar, S., & Mishra, R. (2018). Emerging synergies between Internet of Things and social technologies. *Journal of Global Information Technology Management*, 21(2), 75–80. doi:10.1080/1097198X.2018.1462918

Milton, R., Hay, D., Gray, S., Buyuklieva, B., & Hudson-Smith, A. (2018). Smart IoT and Soft AI. *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*, 1-6. 10.1049/cp.2018.0016

Naito, K. (2017). A Survey on the Internet-of-Things: Standards, Challenges and Future Prospects. *Journal of Information Processing*, 25(0), 23–31. doi:10.2197/ipsjjip.25.23

Poudel, S. (2016). Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security. *Berkeley Technology Law Journal*, 31(2), 997–1022.

Qin, Y., Sheng, Q., Falkner, N., Dustdar, S., Wang, H., & Vasilakos, A. (2016). When things matter: A survey on data-centric internet of things. *Journal of Network and Computer Applications*, 64, 137–153. doi:10.1016/j.jnca.2015.12.016

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and Limitation of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*, 3(9), 369–387.

Razzaq, M., Ali Qureshi, M., Gill, S., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*, 8(6), 383–388.

Sethi, P., & Sarangi, S. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, 2017, 1–25. doi:10.1155/2017/9324035

- Song, M., Zhong, K., Zhang, J., Hu, Y., Liu, D., Zhang, W., ... Li, T. (2018). In-Situ AI: Towards Autonomous and Incremental Deep Learning for IoT Systems. *Proceedings of the IEEE International Symposium on High Performance Computer Architecture (HPCA)*, 92-103. 10.1109/HPCA.2018.00018
- Stake, R. (2005). Qualitative Case Studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research* (pp. 443–466). Thousand Oaks, CA: Sage Publications.
- Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. (2017). A Review of Smart Cities Based on the Internet of Things Concept. *Energies*, 10(4), 1–23. doi:10.3390/en10040421
- Vermesan, O., & Friess, P. (2014). *Internet of Things – From Research and Innovation to Market Deployment*. Aalborg: River Publishers.
- Yang, Y., Wu, L., Yin, L., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250–1258. doi:10.1109/JIOT.2017.2694844
- Yin, R. (2017). *Case Study Research and Applications: Design and Methods*. Thousand Oaks, CA: Sage Publications.
- Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*. Retrieved 2018, October 3, from <https://arxiv.org/ftp/arxiv/papers/1802/1802.03110.pdf>
- Ziegeldorf, J., Morchon, O., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728–2742. doi:10.1002/ec.795

ADDITIONAL READING

- Almeida, F. (2017). Concept and Dimensions of Web 4.0. *International Journal of Computers and Technology*, 16(7), 7040–7046. doi:10.24297/ijct.v16i7.6446
- Altman, M., Wood, A., O'Brien, D., & Gasser, U. (2018). Practical approaches to big data privacy over time. *International Data Privacy Law*, 8(1), 29–51. doi:10.1093/idpl/ix027
- Bao, R., Chen, Z., & Obaidat, M. (2018). Challenges and techniques in Big Data security and privacy: A review. *Security and Privacy*, 1(4), 1–9. doi:10.1002/py2.13
- Gholami, A., & Laure, E. (2016). Big Data Security and Privacy Issues in the Cloud. *International Journal of Network Security & Its Applications*, 8(1), 59–79. doi:10.5121/ijnsa.2016.8104
- Mahmood, A., Zen, H., & Hilles, S. M. S. (2018). Big Data and Privacy Issues for Connected Vehicles in Intelligent Transportation Systems. In S. Sakr & A. Zomaya (Eds.), *Encyclopedia of Big Data Technologies*. Cham: Springer. doi:10.1007/978-3-319-63962-8_234-1
- Matturdi, B., Zhou, X., Li, S., & Lin, F. (2014). Big Data security and privacy: A review. *China Communications*, 11(14), 135–145. doi:10.1109/CC.2014.7085614
- McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1), 1–7. doi:10.1177/2053951716686994

Mgudlwa, S., & Iyamu, T. (2018). Integration of social media with healthcare big data for improved service delivery. *South African Journal of Information Management*, 20(1), 1–8. doi:10.4102ajim.v20i1.894

Tian, Y. (2017). Towards the Development of Best data Security for Big Data. *Communications and Networks*, 9(04), 291–301. doi:10.4236/cn.2017.94020

Zeng, G. (2015). Research on Privacy Protection in Big Data Environment. *Journal of Engineering Research and Applications*, 5(5), 46–50.

KEY TERMS AND DEFINITIONS

Local Area Network (LAN): Computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college.

Metropolitan Area Network (MAN): A network that connects two or more local area networks together but does not extend beyond the boundaries of the immediate town, city, or metropolitan area.

Personal Area Network (PAN): A network typically involving small devices organized around an individual person.

Privacy: Ensuring privacy involves citizens having control over existing information about themselves and exercising this control in a consistent manner with their personal interests and values.

Security: A set of measures taken to protect oneself from any acts of violence, such as attacks, robberies, espionage, sabotage, etc.

Wi-Fi: Abbreviation of wireless fidelity, standard technology for wireless access to local networks. This technology allows electronic devices to be connected to a wireless local area network (WLAN) and Internet using radio waves.

Wide Area Network (WAN): A group of computer networks connected together over a large geographical distance crossing metropolitan, regional, or national boundaries.

Winmax: Technology that allows the expansion of the internet signal at higher speeds over long distances.

Zigbee: Protocol that is employed for PANs and is based on the IEEE 802.15 standard. Even though they are low-powered, Zigbee devices can transmit data over long distances by passing data through intermediate devices to reach more distant ones, creating a mesh network.

ENDNOTES

¹ <https://www.docker.com>

² <https://kubernetes.io>

Cybercrime and Private Health Data: Review, Current Developments, and Future Trends

4

Stavros Pitoglou

 <https://orcid.org/0000-0002-5309-4683>

National Technical University of Athens, Greece & Computer Solutions SA, Greece

Dimitra Giannouli

Computer Solutions SA, Greece & University of Leeds, UK

Vassilia Costarides

Institute of Communication and Computer Systems (ICCS), Greece

Thelma Androutsou

National Technical University of Athens, Greece

Athanasios Anastasiou

National Technical University of Athens, Greece

INTRODUCTION

One significant benefit of the development of information technology is its positive impact on the health sector. Over the last years, the use of electronic patient records has illustrated rapid expansion. The advancements in health information technology, the limited potential of the traditional processes and the need for flexible access to health information, have promoted new paradigms and as a result, personal health record (PHR) systems, empowering both patients and healthcare providers, present a constantly evolving area for research, development, and implementation (Genitsaridi, Kondylakis, Koumakis, Marias, & Tsiknakis, 2015). The technological challenges intertwined with the increasing adoption of such tools and platforms are optimally addressed with the rise of Cloud Computing (Martens & Teuteberg, 2012) which is formally defined as “*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction*” (Mell & Grance, 2011). Promising coherence and economies of scale through the ability of robust sharing of computational resources, Cloud Computing has been a continuously evolving sector over the last decades (Guzek, Bouvry, & Talbi, 2015).

Furthermore, the availability of large medical datasets for secondary purposes such as research has become a powerful tool for producing knowledge and information, leading the medical and health care sector to a new, more personalized level. Large-scale biomedical databases are created and continuously enriched for research purposes while providing the right tools for handling and analyzing their content (Dankar & Al Ali, 2015). Researchers using personalized patient medical data have the ability to present valid and reliable data, to reuse existing data, and to compare the results of their study with similar ones based on the same database (Emam, 2013).

DOI: 10.4018/978-1-5225-9715-5.ch052

As the type of data shifts toward electronic records and large datasets are made accessible via distributed networks and the world wide web, hospitals, and other health providers increasingly suffer from data breaches whose nature likewise shifts toward electronic means, such as hacking (Spitzer, 2018). A data breach is “*an impermissible use or disclosure that compromises the security or privacy of the protected health information and is commonly caused by a malicious or criminal attack, system glitch, or human error*” (Bai, Jiang, & Flasher, 2017). Breaches can be conducted by a variety of ways, including credential-stealing malware, an insider who either purposefully or accidentally discloses patient data, or lost laptops and smart devices (Center for Internet Security, 2018).

Healthcare industry is highly targeted by cybercriminal organizations and individual hackers, as, according to research, an individual’s medical data, are 20 to 50 times more valuable to cybercriminals and black market than other types of targeted information, e.g., personal financial data, credit card details, social security numbers, etc. (Center for Internet Security, 2018). Therefore, cybercriminals have higher incentives to target databases with medical content in order to sell or exploit the sensitive information for their own personal gain (Center for Internet Security, 2018). In this context, it is not a coincidence that the biggest recent data breaches have seized health care records as the prize.

Access to highly sensitive medical information which is exposed through data breaches, gives cybercriminals the opportunity to commit identity theft, medical fraud, extortion, and the ability to illegally obtain controlled substances (Kruse, Frederick, Jacobson, & Kyle, 2017). More specifically, patient records can be used for various types of financial gain, including (Boden, 2018):

- sale on the Dark Web
- fraud commitment (tax, insurance frauds)
- extortion of people whose disclosure of illness could provoke public relationships problems and difficulties in their working environment
- targeted phishing campaigns against individuals whose records were leaked

In the recent years there is an uptick in attacks against health care systems due to a variety of factors, including low organizational vigilance, inadequate and poorly trained staffing, insufficient technology investment and funding for information technology security, all these combined with the potential value of healthcare data as compared with other industries (Gordon, Fairhall, & Landman, 2017).

CURRENT TRENDS

In the past years, the growth of healthcare data breaches in both size and frequency was remarkable, with the largest breaches having an impact on millions of people (Chideya, 2015). In the years 2016-2017, approximately 90 percent of healthcare providers were faced with data breaches and cyber-attacks were up 125 percent since 2010 (Kruse et al., 2017). Currently, in the U.S., the number of individuals affected is estimated to be more than half of the total population.

A data breach outside of the USA that is worth mentioning is the Singapore Health cyberattack. The personal particulars of almost 1.5 million patients, including that of the country’s Prime Minister, were stolen from the database. The data include both demographic and medication records (Singhealth et al., 2019). On the other hand, National Health Service (NHS) was on the top of the list for serious data breaches in 2014. The percent of severe data breaches that were reported to the Information Commis-

sioner's Office was highly increased, while most of the incidents were related with human error and deficient data handling and not with technical reasons (Gilbert, Goldstein, & Hemingway, 2015).

Following the development of a market for stolen data and related hacking skills, hospitals and other healthcare providers have become popular targets for hackers and cybercriminals. As an example, in June 2016 a hacker offered for sale in "Real Deal" dark web marketplace more than 60.000 medical records from three different systems, one of which was an entire electronic health record, including screenshots. In the same month, cyber-attacks disclosed more than 11 million healthcare records (Chideya, 2015; Koczkodaj, Mazurek, Strzałka, Wolny-Dominiak, & Woodbury-Smith, 2018).

Table 1 presents the top 10 biggest healthcare data breaches, according to the U.S. Department of Health and Human Services Office for Civil Rights. The breaches are illustrated in descending order, regarding the number of individuals affected.

VULNERABILITIES - ATTACK METHODS

Social Engineering

Regardless of how strongly the security is maintained on the systems' level, human intervention always should be considered as the weakest link in the security chain. Social engineering is a set of techniques used by cybercriminals, that allows the access to buildings, systems or data by exploiting human psychology, or, defined from a different angle, *"the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity"* (Junger, Montoya, & Overink, 2017).

Used as a technique to penetrate any type of system, exploiting humans related to it rather than vulnerabilities in the system itself, Social Engineering Attacks are rather powerful because they operate on a level such that there is no hardware or software that can prevent or even help defend against them (Koyun & Al Janabi, 2017). Although the nature of this attack is not considered as technical, social engineering methods are widely used by cybercriminals. These tactics, which are based on the manipulation of people's psychology by exploiting their possible lack of awareness and the tendency to trust easily are often far more effective and faster than software hacking. (Criddle, 2017). So, social engineers may use a combination of collected data regarding their victims in order to make them believe that they are authorized users, for example, IT employees, and reveal to them confidential information such as passwords. It is a fact that most people want to be kind and courteous and are trained to be compliant, especially in a work environment. If a potential intruder calls up as an angry executive and claims that he wants to know, for example, why nobody has taken care of a specific routing number and account number which were supposed to be changed, with a sense of urgency to it, employees tend to obey immediately.

A social engineering attack can be accomplished by a variety of ways; phone, web, email, USB drives to name such a few. Most common social engineering categories include:

- **Phishing** is the most widely known social engineering attack and is normally executed via emails and social media. Victims of such an attack usually receive emails or text messages from an entity that either they trust or seems to be legitimate, for example, a friend, their bank or university. These messages often contain malicious links that redirect recipients to websites which can either trick them into revealing sensitive information or automatically download malware which can

Table 1. Top Healthcare Data Breaches in the U.S. ^(a) Lower rank number denotes larger impact ^(b) Estimated number of affected individuals (in millions) ^(c) After unusual activity was detected in Banner's servers a cybersecurity firm conducted further investigation that revealed two attacks. ^(d) The protocols that were supposedly enacted after a previous breach in 2009 were not activated at the affected offices by 2013. ^(e) The breach affected anyone who had received treatment at one of CHS's network-owned hospitals in the past five years or had been referred to CHS by an outside doctor during that period. ^(f) The data were not encrypted. ^(g) The breach involved active and retired military personnel as well as their families. ^(h) After a rash of cyber-attacks targeting healthcare data in early 2015, ordered a forensic investigation of Excellus systems took place after a peak of attacks in 2015. The discovered breach extended to December 2013. ⁽ⁱ⁾ The biggest recorded data breach to date. Source: (Lord, 2018a)

Rank ^(a)	Data Breach	Affected Individuals ^(b)	Month(s)/Year	Data Compromised
10	NewKirk Products	3.47	August 2016	• Primary Care Provider Information, • Medicaid ID Numbers, • Names (including those of dependents), • Dates of Birth, • Premium Invoice Information, • Group ID Numbers.
9	Banner Health ^(c)	3.62	August 2016	• Names, • Passwords, • Credit Card Numbers and Expiration Dates, • Addresses, • Birth Dates, • Social Security Numbers, • Patient Records
8	Medical Informatics Engineering	3.9	July 2015	• Names, • Social Security Numbers, • Phone Numbers, • Mailing Addresses, • Dates of Birth, • Diagnoses
7	Advocate Health Care ^(d)	4.03	August 2013	• Medical and Claim Data
6	Community Health Systems ^(e)	4.5	April-June 2014	• Social Security Numbers, • Dates of Birth, • Phone Numbers • Physical Addresses.
5	University of California, Los Angeles Health ^(f)	4.5	July 2015	• Patient Records
4	TRICARE ^(g)	4.9	September 2011	• Social Security Numbers, • Phone Numbers • Home Addresses
3	Excellus BlueCross BlueShield ^(h)	10+	September 2015	• Medical Data, • Social Security Numbers • Financial Information.
2	Premiera Blue Cross	11+	January 2015	• Bank Account Numbers, • Social Security Numbers, • Dates of Birth, • Claims Information.
1	Anthem Blue Cross ⁽ⁱ⁾	78.8	January 2015	• Names, • Social Security Numbers, • Home Addresses • Dates of Birth. • Sensitive Medical Information

encrypt useful files of the system (ransomware attack). The targeted phishing attacks are usually the most successful because criminals collect personal information from customers and use it in order to create more convincing emails. For example, criminals can imitate effectively emails from online shops just by mentioning the customer's name and the products they purchased. The more information an attacker has collected about the target, the better he can imitate emails from trusted entities. According to an experiment about phishing attacks, using data from social media, individuals are 4.5 times more likely to get deceived from a message sent from a contact they trust than from standard phishing attacks. It is important to be mentioned, that at the Corps of Cadets at West Point 512 students received a phishing email which concerned a problem with their grades. The vast percentage of 80% opened the link embedded in the email. (Junger et al., 2017).

The majority of criminals who perform phishing attacks aim to gain access to personal information, such as age, names, addresses, credit card details, social security numbers, and health records. Phishing methods exploit fear in order to deceive users and make them react thoughtlessly. For instance, criminals can send victims via email that the password for a service will be expired and they should update it within 24 hours, otherwise they will lose their account.

- **Pretexting** is another social engineering category, where attackers try to divulge victim into trusting them and give them access to either sensitive or non-sensitive personal information, by generating an effective pretext, a scenario that seems plausible or a story that cannot be doubted. Pretexting attacks aim to build a notional trust relationship with the target, in contrast to phishing tactics, which take advantage of emotions such as fear in order to manipulate individuals. (Bisson, 2015).
- **Baiting attack** is one of the simplest social engineering methods since, usually, all that it involves is an external storage device. This kind of attack exploits people's natural curiosity and its main difference from the other social engineering methods is that hackers use to tempt their victims by offering them an item or a service. For example, targets may be offered services like free movies or music, if they submit their login credentials to a given website in return. (Bisson, 2015).

Concerning baiting attacks through physical media, criminals often leave intentionally a device that contains malicious software in a public place, where potential victims can easily find and use it. This place could be a parking lot, a park, the corridors of a company, or even a pavement. If a number of individuals find such a device and plug it into their computers, curious to discover what will happen, baiting attack will achieve its purpose. In 2006, the founder of Secure Network Technologies Inc conducted an experiment in order to evaluate the security level of a client. His team scattered a significant number of malware-infected USB devices around the company's parking lot. Many of the company's employees plugged the devices into their computers and, as a result, they unintentionally activated a keylogger which exposed their login information.

- **Quid pro Quo attacks** are similar to baiting attacks, as they deceive people into believing that they will receive a service or a good if they provide information. In contrast to baiting, which usually relates to an item, quid pro quo attacks frequently use provision of services in order to attract victims. One typical instance of quid pro quo attack includes criminals who call targets and pretend to be IT experts who will help victims fix their software problems if, for example, they

Table 2. *Top Web Application Vulnerabilities. Selected from (“Top 10-2017 Details About Risk Factors - OWASP,” 2017)*

Risk	Exploitability	Prevalence	Detectability	Impact
Injection	Easy	Common	Easy	Severe
Broken Authentication	Easy	Common	Average	Severe
Sensitive Data Exposure	Average	Widespread	Average	Severe
Broken Access Control	Average	Common	Average	Severe
Security Misconfiguration	Easy	Widespread	Easy	Moderate
Cross-Site Scripting (XSS)	Easy	Widespread	Easy	Moderate
Vulnerable Components	Average	Widespread	Average	Moderate
Insufficient Logging Monitoring	Average	Widespread	Difficult	Moderate

disable their antivirus program and install some updates on their computer, which is, in fact, malicious software. (Bisson, 2015).

- In **tailgating attacks**, fraudsters try to gain access to a restricted area, for example, a company, by exploiting an authorized person such as an employee. Frequently, criminals pretend to be delivery drivers or couriers and ask from the employees to hold the door for them. Tailgating is not effective in work environments such as large companies where all individuals who require to enter the building are obliged to use their personal card. (Bisson, 2015)

Web Application Security Risks

As an increasing number of patient data are made available to both patients and health professionals through web application interfaces, the “innate” security, which depends on careful and responsible application development processes, becomes of crucial importance. Vulnerabilities that derive from developers’ sloppiness or lack of knowledge present a favorite hacking target, and they are, more often than not, easier targets to exploit compared to system level processes, which are typically hardened by default. There are numerous known vulnerabilities on that level. One of the most comprehensive lists, compiled by Common Weakness Enumeration (CWE), a “community-developed list of common software security weaknesses,” contains no less than 716 items (“CWE - CWE List Version 3.1,” 2017).

Open Web Application Security Project (OWASP) is an international organization “dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.” As part of their foundation statement they “advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas” (“About The Open Web Application Security Project - OWASP,” 2018). Among other activities, OWASP conducts worldwide research about the most prevalent web application vulnerabilities that allow successful attacks to internet users’ privacy and security. Table 2 presents a selection of OWASP’s top 10 vulnerability list, adapted to the specific nature of HealthCare systems, along with threat assessment classifications.

More specifically:

- **Injection:** Injection flaws occur when, under any circumstance, the user provided command or query data is allowed to be executed on the interpreter level, thus giving an attacker the opportunity to perform unintended commands without proper authorization. Given that this type of vulnerability is very common, particularly in legacy code, injection attacks are on the rise and can sometimes lead to complete host takeover. In the most typical scenario, a hacker executes a SQL query from the Internet to perform an operation on the recipient's database and transfer data back to themselves (Harries & Yellowlees, 2013).
- **Sensitive Data Exposure:** Data Attackers can steal or modify weakly protected data when there is no extra protection such as adequate encryption both when stored (at rest) and during the communication of the server with the user's client, e.g., internet browser (in transit). Often there is no encryption used whatsoever. However, even when crypto is employed, vulnerabilities could emerge from the use of weak and/or obsolete algorithms, as well as wrongly implemented key generation, exchange, and cipher usage.
- **Broken Authentication:** If application procedures related to authentication and session management are not implemented correctly, which is often the case, this allows attackers to assume other users' identities temporarily or permanently, making use of compromised passwords, keys, or session tokens. Common attack methods used are credential stuffing (as there are publicly available databases with millions of valid credential combinations as well as default administration account lists), dictionary/rainbow attacks, and automated brute force. Also, poorly implemented session management is a favorite target, as it lies in the center of authentication and access control mechanisms and exists in all stateful applications.
- **Broken Access Control:** Such flaws occur when an attacker can gain unauthorized access to functionality and/or data, due to poorly enforced restrictions on what authenticated users can do. Failure to implement effective access control, that is to enforce policies to prevent users from acting outside of their assigned permissions, can allow perpetrators to access administrative/privileged functions or to act on behalf of other users, increasing the probability of data disclosure, modification or destruction.
- **Security Misconfiguration:** This is one of the most commonly seen issues and can be observed at all levels of the application stack (network, platform, web/application/database server, virtual machines, containers, and storage). Lack of diligence and/or knowledge can result to a number of insecure configurations (default accounts with unchanged credentials, administrative or development access routes –e.g., ports, services- forgotten active and unprotected, etc.), allowing the attackers to relatively easily access sensitive functionality and data.
- **Cross-Site Scripting (XSS):** XSS flaws occur whenever malicious HTML and/or Javascript code included in user input is not properly handled (validated and/or escaped) and is allowed to be part of the web page output or to be executed in the victim's internet browser. This can happen during the same session (Reflected XSS), at a later time by another user (Stored XSS) or by exploiting dynamically structured web applications (DOM XSS). Executing hostile code via XSS in the user's browser can result in user session hijacking, defacing, or redirection the user to attacker-controlled sites.
- **Using Components with Known Vulnerabilities:** More often than not, development teams working with component-rich applications fail to keep track of which components they use, as well as keeping them updated and properly patched. Many of the large recorded breaches have

relied on exploiting known vulnerabilities in third-party components, as, in most of the cases, they share the same execution privileges with the main application.

- **Insufficient Logging/Monitoring:** This flaw is the foundation of nearly every recorded major incident as it provides attackers with valuable time to achieve their goals before being detected. Data from 2016 suggest that the detection and identification of a breach took, on average, more than 190 days. Given the privilege of time, attackers can dig deeper, pivot to adjacent systems, and introduce new vulnerabilities. On the contrary, timely response to a security incident can, most of the times, reduce dramatically the final impact.

Database Anonymity Issues

Patient privacy must be one of the main considerations when attempting to distribute and share medical data for secondary purposes. Research has shown that datasets that may seem completely anonymized are prone to specific types of attacks that can result in one or more physical persons' identification. The identifiers through which an individual's identity may be revealed can be divided into two categories (El Emam, Rodgers, & Malin, 2015):

- **Direct Identifiers:** they include data allowing the immediate identification of the holder, such as the name, the identity card number, the social security number, etc.
- **Indirect Identifiers or Quasi-Identifiers:** They include characteristics such as age, gender, occupation, residence, etc., which do not directly identify an individual, but their combination may lead to revealing identity and violating personal privacy. Indirect identifiers may also include the sub-category of sensitive attributes, which are not public data and can be harmful or lead to stigmatization when associated with a particular person. Such features include drug and intervention codes, as well as certain diseases (Eze & Peyton, 2015). The attack may involve either the identification or attribute disclosure. During the identification disclosure, the attacker uses the indirect identifiers of an anonymous record to associate them with a particular person. During the attribute disclosure, on the other hand, the perpetrator of the attack can infer some sensitive information about a person even if he/she cannot identify and find which unique record corresponds to him/her. A third and less frequent form of attack is membership disclosure, which is a probabilistic measure of the presence or absence of a person in a data set (Eze & Peyton, 2015).

Improper handling of these identifiers or their combinations can give attackers the opportunity to re-identify parts of the respective datasets, which, most of the times, given their medical research purpose, contain extremely sensitive data.

Attacks That Do Not Disclose Sensitive Data

Although the attacks that aim to the disclosure of personal health information are far more worrisome, cyber-attacks that do not necessarily result in data breaches, can potentially have a significant impact in terms of cost, loss of trust, etc. (Gordon et al., 2017) The most common types of these attacks are:

- **DoS (Denial of Service) Attacks:** Criminals can use a variety of methods in order to harm health care providers. A widely known category of attacks that are used against health care systems is Denial of Service (DoS) attacks which flood systems with a vast amount of network traffic in order to disable them. This kind of attacks in the healthcare sector may be dangerous or even fatal as they may affect operations such as surgical procedures or reporting of lab results by rendering hospital care systems unusable. (Gordon et al., 2017)
- **Ransomware:** Ransomware attacks have as main characteristic the encryption of selected files in an information system, for example, a patient database, and the request of a fee, usually in cryptocurrencies such as Bitcoin, in order to give victims, the key to regaining access to their files. (Gordon et al., 2017) Restricted files are usually highly significant for the smooth operation of hospital procedures, and as a result, hospitals are forced to pay the criminals. Otherwise, there is the possibility of losing vital data. Even if organizations keep daily backups of their files, there is always the risk of losing information if they restore from a backup after a ransomware attack.

The creation of ransomware dates back to 1989 when Dr. Joseph Popp used malware-infected floppy discs which distributed to attendees of the WHO (World Health Organization) conference that focused on AIDS research. Although Dr. Popp ended up in prison, his creation inspired many aspiring cyber attackers. A recent example of a ransomware attack is the WannaCry attack in 2017, which had an impact on NHS. Concerning the ransom fee, most of the times, it seems inferior to the consequences that will provoke a potential data loss to an organization, which may include profit loss and damaged security reputation. However, even payment does not ensure access to encrypted files, as ransomware victims are totally dependent on the attacker's reliability. (Gordon et al., 2017) *'Ransomware exposes and exploits the vulnerabilities of 21st-century information technology (IT) infrastructure'* (Kruse et al., 2017)

Monetization Routes

The main motivation for conducting a major attack to gain access to large datasets of private sensitive information is profit, thus, once the data acquisition is achieved, the next perpetrators' move, predictably, is the effort of monetization. Most of the times, the preferred method includes black market structures that utilize the anonymity and counter-tracking environment provided by dark/deep web and cryptocurrency, which are briefly presented in the subsequent sections.

Deep/Dark Web

What is known as Deep Web, Deep Net, Invisible Web, or Dark Web (Weimann, 2016), is the non-indexed by standard search engines content of the World Wide Web. If the Internet is considered as a multi-tiered structure, only the top tier, i.e., the surface web, can be accessed with the regular search engines that are commonly used (such as Google). The rest, the deepest tiers, which are the essential content of the Deep Web, is a wealth of information. Searching the internet has been compared to *"dragging a net across the surface of the ocean: a great deal may be caught in the net, but there is a wealth of information that is deeper and therefore missed"* (Bergman, 2001). In the early days of the Internet, as the size of information was not immense, it was indexed and accessed in an easier way. However, as its use inflated, conventional search engines are proving insufficient for searching and indexing dynamic pages, whereas they are adequate for static web pages. Dynamic pages can be accessed through specific

and targeted queries and programs, while static pages are linked to other pages on the internet, therefore the name “Invisible” web.

The Deep Web is inaccessible by conventional means, with its contents hidden or often blocked. Although its size can't be measured, it has been estimated (Bergman, 2001) that public information on the Deep Web is currently 400 to 550 times larger than the commonly defined web, although there have been since more moderate estimations (Cox, 2015).

A segment of the Deep Web is the Dark Web that contains information that is considered generally illegal, antisocial and it is possible to access it only through specialized browsers, created for this specific task. Examples of such pages may include illegal paraphilia, leaks on unauthorized information, financial trails on money laundering, frauds, identity thefts, illegal transactions, trafficking, etc. Associated with the Dark Web is the rise of relevant sub-cultures (Bartlett, 2015) such as social media rapists, crypto-anarchists, transhumanists, traffickers, etc. The Dark Web can be visited by all Web users, by software such as Tor, free software for enabling anonymous communication. The name is derived from an acronym for the original software project name “The Onion Router.” Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Another relevant software is the Invisible Internet Project (I2P), which is an anonymous network layer that allows for censorship-resistant, peer to peer communication (Ali et al., 2016; Astolfi, Kroese, & Van Oorschot, 2015). These anonymous connections are implemented by encryption (end-to-end) of the user's traffic and delivery of the information through a volunteer-run network of roughly 55,000 computers distributed around the world. Given the high number of possible paths the traffic can transit, a third party watching a full connection is unlikely to successfully gather information about the communication. The software that implements this layer is called an “I2P router”, and a computer running I2P is called an “I2P node”. I2P is free and open source and is published under multiple licenses. The overall principle is that whatever tool a visitor uses, one must know where exactly to find the website, by its Uniform Resource Locator. Once inside the Dark Web, communication means include secure email, Web Chatting, or Tor-hosted Personal Messaging (PM).

Cryptocurrency

Cryptocurrencies use decentralized control versus centralized digital currency and the traditional banking system. They are transferred between peers, and they are confirmed in a public ledger with a process that is called mining (Dziembowski, 2015).

More specifically, these public ledgers are storing all confirmed transactions, from the beginning of each cryptocurrency's creation. Information regarding the cryptocurrency's owners is encrypted, as well as the legitimacy of record keeping. When there is a transaction, meaning a transfer of funds between digital wallets, this is submitted to the abovementioned public ledger, while confirmation is pending. In order to provide mathematical proof and a legitimate link between the owner of the wallet and the relevant transaction, an electronic signature is used, which is an encrypted piece of data. Then ‘mining’ confirms the transactions, and they are added to the ledger. The mining process is what essentially gives value to the cryptocurrency and is its proof-of-work system. Cryptocurrency mining, or crypto mining as is otherwise known, is the process of transactions verification, by cryptocurrency miners, who are responsible for ensuring the authenticity of information and updating the blockchain. Cryptominers, compete with each other, in solving complex mathematical problems and the first one to

find the solution, authorizes the transaction, while being rewarded for the service provided by earning small amounts of cryptocurrency.

Bitcoin, described as the currency of the Dark Web, was proposed in 2008 as an alternative and independent currency by S. Nakamoto (Nakamoto, 2008). Currently (Hurlburt, 2017), it is being rapidly replaced by Monero, a private, digital currency that is offering mechanisms that prevent the indirect tracing of those that are conducting transactions (Amsterdam, 2018; Noether, 2016).

COUNTERMEASURES

A countermeasure is a procedure that reduces vulnerability by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. A set of policies concerned with information security management has been developed to manage, according to risk management principles, the countermeasures in order to accomplish a security strategy set up following rules and regulations applicable in the world. Below the various existing protocols of preventing any misuse of healthcare data are described.

Government Regulations

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA (Health Insurance Portability and Accountability Act) is a United States legislation which provides guidelines regarding the security of sensitive medical information and enacted in 1996 by Bill Clinton (HIPAA, 2018)

Before the activation of HIPAA, there were no healthcare security guidelines or requirements with a focus on the protection of personal health data. The existence of such legislation has become vital during the last few years when the number of cyber-attacks targeting healthcare providers, which resulted in health data breaches illustrated a rapid increase.

HIPAA is organized into five (5) separate sections or “Titles” (“HIPAA (Health Insurance Portability and Accountability Act) | whatis.com,” 2017):

- **Title I, “HIPAA Health Insurance Reform.”** This section refers to new employees’ medical insurance coverage. According to this title, employers should allow new employees’ coverage to be uninterrupted regardless of any pre-existing conditions or health problems.
- **Title II, “HIPAA Administrative Simplification.”** When mentioning HIPAA compliance, most people mean adhering to HIPAA Title II. This part of the legislation sets the national standards for processing electronic healthcare transactions. It also requires the implementation of secure electronic access to personal health information, and all healthcare organizations’ activities must be in accordance with privacy rules.
- **Title III, “HIPAA Tax-Related Health Provisions.”** In the presented title, tax-related provisions are concerned.
- **Title IV, “Application and Enforcement of Group Health Plan Requirements.”** This section additionally provides information concerning insurance reform and provisions for individuals who request subsection to continuous insurance coverage.

- **Title V, “Revenue Offsets.”** The presented title provides regulations concerning company-owned life insurance and the behaviour towards individuals who lose their U.S. citizenship for income tax purposes.

All HIPAA-covered entities, including healthcare clearinghouses and providers, are affected by HIPAA privacy rule. When a HIPAA-covered entity uses a contractor or a non-workforce member to accomplish “business associate” activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement. This contract imposes specific safeguards on the PHI (Protected Health Information) that the business associate uses or discloses. (“Summary of the HIPAA Security Rule | HHS.gov,” 2013)

One of the most important aims of the Security Rule is to protect the privacy of individuals’ sensitive medical information while allowing covered entities to improve the quality and efficiency of patient care by adopting new technologies. Due to the extended diversity of the health care marketplace, it should be ensured that the flexibility and scalability of the design of Security Rule would allow covered entities to *“implement policies, procedures, and technologies that are appropriate for the entities particular size, organizational structure, and risks to consumers’ e-PHI (Electronic Protected Health Information)”*. (“Summary of the HIPAA Security Rule | HHS.gov,” 2013) Protected Health Information is the definition used by HIPAA to define the type of patient information that falls under the jurisdiction of the law. Billing information from doctors, blood test results, phone records, and emails to doctors which concern a health problem or a medication the patient needs are only a few examples of PHI (“Protected Health Information (PHI) - TrueVault,” n.d.). However, there are cases, such as employment records, that are not considered as PHI, and Privacy Rule does not support cover entities’ individually identifiable health information. (“HIPAA Privacy Rule and Its Impacts on Research,” 2005)

Data that have undergone the process of de-identification, *“a process that is applied to a dataset with the goal of preventing or limiting informational risks to individuals, protected groups, and establishments, while still allowing the production of aggregate statistics.”* (Garfinkel, 2016) are no longer subject to the provisions of the HIPAA Rule.

The fine for a potential HIPAA violation can reach \$50,000 per violation, while the annual maximum for repeat violations reaches the \$1.5 million. Covered entities and individuals who are accused of intentional obtainment or disclosure of PHI in violation of the HIPAA Privacy Rule, can be fined up to \$50,000 and receive up to one year in prison. If the HIPAA Privacy Rule is violated under false claims, the penalties can reach the amount of \$100,000 and the number of 10 years in prison. (“HIPAA (Health Insurance Portability and Accountability Act) | whatis.com,” 2017)

HITECH Act (Health Information Technology for Economic and Clinical Health)

On February 17, 2009, the Office for Civil Rights enacted the Health Information Technology for Economic and Clinical Health (HITECH) in order to “strengthen the privacy and security” portions of HIPAA regulations. The HITECH program authorized the Office of the National Coordinator (ONC) to “manage and set standards for the stimulus program”. (Hazard, 2017). It was created in order to prompt the implementation of electronic health records (EHR) and promote the application and the meaningful use of information technology in the area of the United States. *“HITECH Act was an ambitious effort to modernize the Health IT infrastructure to keep up with the demands of the 21st century.”* (Washington, DeSalvo, Mostashari, & Blumenthal, 2017)

The HITECH Act expanded the privacy and security protections introduced by HIPAA by increasing the potential legal liability for non-compliance and providing more rigorous enforcement. (“What is the HITECH ACT? | What HITECH Compliance Means,” 2009)

One of the issues that HITECH had to confront at the beginning was the generation of the interoperability in such an environment which characterizes from a mixed public and private economy and a sharing federal and state governing system. This kind of problems remained unsolved until today. Short-term priorities and experimentation with various models for engaging private providers, states, and health systems, constituted the main focus of the HITECH Act during the initial years of its enactment. (Gold & McLAUGHLIN, 2016)

HITECH extended the HIPAA security provisions and penalties beyond covered entities to include business associates. In the original HIPAA rule, it was stated that cover entities should get assurance from business associates they share information with, that they will protect individuals’ personal information. However, most of the covered entities neglected this rule.

HIPAA violation penalties can extend up to \$250,000, with repeat violations which remain uncorrected reaching \$1.5 million. (“What is the HITECH ACT? | What HITECH Compliance Means,” 2009; Withrow, 2010)

GDPR (General Data Protection Regulation)

The minimum guidelines concerning data processing in the EU were set by Data Protection Directive 95/46/EC until spring 2018 when it was replaced by General Data Protection Regulation (GDPR) as the primary law regulating how companies protect EU citizens’ personal data. GDPR, which was voted by the European Parliament and Council in April 2016, reinforces and clarifies natural persons’ rights in regards to the processing and free movement of natural persons’ personal data, especially in IoT healthcare applications. (“Data protection in the EU | European Commission,” 2016; Pulkkis, Karlsson, Westerlund, & Tana, 2017). GDPR regulation refers to every European Union member state and has as main purpose to protect effectively the personal information of European citizens. Through GDPR, a uniform data security law is imposed on all members of EU, so that each member state no longer needs to write its own data protection laws and laws are consistent across the entire EU. Except for EU members, GDPR regulation also concerns any company in the world that operates in the EU by marketing goods or services to EU residents. (Lord, 2018b)

Some of the GDPR guidelines are referred below:

- Subjects must allow the processing of their personal information
- Collected data should be subjected to an anonymization process in order to protect the data owner’s privacy
- Natural persons should receive information about who owns the data if a data breach takes place
- The transfer of data across borders should be secure
- Companies should add to their human resources a data protection officer (DPO) to supervise GDPR compliance

GDPR provides individuals with a notable number of rights, as they have the ability to require the revelation or deletion of their personal data from the companies that hold them. Moreover, with GDPR, there is no need to launch separate actions in each jurisdiction, as regulators, for the first time, will be able to work in concert across the EU. (Hern, 2018)

A company found in violation of the Regulation may confront significant fines and compensation fees to data subjects, which may be up to 2% or 4% of total global annual turnover or €10m or €20m, whichever is greater. (“GDPR Article 83 – General conditions for imposing administrative fines,” 2016)

Act on the Protection of Personal Information

The Act on the Protection of Personal Information is the key legislation governing the collection, storage, and use of personal information in Japan. It applies to business operators that handle personal information and has a comparable level of data protection to that of the European Union (Orito & Murata, 2005). Among others, the Act specifies the circumstances under which personal data can be collected, stored, and processed:

Processing: A business operator governed by the Act on the Protection of Personal Information must specify the purpose of use for personal information it handles (to the extent possible) and comply with the following rules:

- it must not change the purpose of use beyond a scope which has a reasonably substantial relationship with the original purpose of use; and
- it must not use the personal information beyond the scope necessary to achieve the purpose of use, without obtaining the individual’s prior consent.

Collection: The following restrictions apply to the collection of personal information by business operators governed by the Act on the Protection of Personal Information:

- proper acquisition – a business operator must not acquire personal information by deception or other wrongful means;
- notice of purpose of use at the time of acquisition – once a business operator has acquired personal information, it must notify the individual of or publicly announce the purpose of use, unless it has already been publicly announced or one of the following applies:
- such notification or public announcement would likely cause harm to the life, body, property, rights or interests of an individual or third party;
- such notification would likely harm the business operator’s rights or legitimate interests;
- cooperation with a state agency, local government or third party commissioned by a state or local agency is necessary to conduct certain affairs specified by laws and regulations and the notification, or public announcement of the purpose of use would likely impede the execution of such affairs; or
- the purpose of use is evident from the circumstances around the collection of personal information.

The guidelines issued by the Personal Information Protection Commission (PPC) include examples of how business operators can make such public announcement – namely, by posting it on their websites or displaying it in an easily viewable location within their places of business.

Business operators must not obtain sensitive information without the individual’s prior consent. Sensitive information means personal information comprising a principal’s race, creed, social status, medical history, criminal record, the fact of having suffered damage as a result of a crime, or other descriptions described by the cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

Storage: Business operators governed by the Act on the Protection of Personal Information must take security control measures in regards to personal data. The act imposes a broadly stated obligation on business operators to “take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the Personal Data.” The act provides no concrete measures to satisfy this requirement. However, it is generally understood that such security control measures include:

- organisational measures;
- employee-related measures (e.g., personnel training);
- physical measures; and
- technical measures.

Specific actions to be taken for each type of measure are stipulated in the various guidelines issued by the PPC.

Preventing Social Engineering

Despite the variety of technical vulnerabilities and attack methods, the weakest link in security infrastructure is people, as unintentional negligence remains the biggest risk. Healthcare Organizations should raise awareness and regularly educate their employees: Security through education is the first, main, and most effective mitigation policy. If people aren’t educated about the types of attacks being used, they have a very low possibility to defend against them. To this end, a security policy must be written and backed up by adequate awareness training. The policy must encompass clear sets of guidelines of response to any given situation. *“Absent such guidelines, employees will default to actions they perceive as helpful, which often means giving away information they shouldn’t”* (Olavsrud, 2010).

Securing Web Applications

Mitigating the risks of a perpetrator exploiting flaws in one’s web application stack is not to be considered a trivial task, as it requires vigilance and deep up-to-date knowledge through all levels and phases of the application development process. To this end, there exist well documented and continuously updated bodies of guidelines, like the one maintained by OWASP. Their recommended courses of action, regarding the vulnerabilities mentioned in a previous section, are presented in Table 3.

Preserving Anonymity

Taking into consideration the difficulties described above regarding the high cost that a possible online attack and interception of personalized medical data may entail, the imperative need for anonymization of medical information (El Emam & Arbuckle, 2013) arises. Data anonymization is the process of encrypting or removing information from a data set so that the identification of the persons is not anymore feasible. Thus privacy protection is achieved. From a legal point of view, anonymized data cease to be personal data, and as a result, their disposal does not require approval and consent (Emam, 2013). However, the process of anonymization should be done in a strict and methodical form in order to minimize the risk of disclosure. As mentioned above, the General Data Protection Regulation (GDPR) in Europe, along with the United States of America’s Health Insurance Portability and Accountability Act (HIPAA) and

Table 3. Recommended preventive actions for the mitigation of Web Application vulnerability risks

OWASP recommendations to developer teams	Related Vulnerability
Use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs). Note that even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().	Injection
Use positive or “whitelist” server-side input validation.	
For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter.	
Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.	
Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks.	Broken Authentication
Do not ship or deploy with any default credentials, particularly for admin users. Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords.	
Align password length, complexity, and rotation policies with NIST 800-63 B's (Grassi et al., 2017) guidelines in section 5.1.1 for Memorized Secrets or other modern, evidence-based password policies.	
Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes.	
Limit or increasingly delay failed login attempts. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.	
Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL, be securely stored and invalidated after logout, idle, and absolute timeouts.	Sensitive Data Exposure
Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.	
Apply controls as per the classification.	
Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.	
Make sure to encrypt all sensitive data at rest.	
Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.	
Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and security parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).	
Disable caching for a response that contains sensitive data.	
Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt, or PBKDF2.	
Verify independently the effectiveness of configuration and settings.	Broken Access Control
Access control is only effective if enforced in trusted server-side code or server-less API, where the attacker cannot modify the access control check or metadata.	
With the exception of public resources, deny by default.	
Implement access control mechanisms once and re-use them throughout the application, including minimizing CORS usage.	
Model access controls should enforce record ownership, rather than accepting that the user can create, read, update, or delete any record.	
Unique application business limit requirements should be enforced by domain models.	
Disable web server directory listing and ensure file metadata (e.g., .git) and backup files are not present within web roots.	
Log access control failures, alert admins when appropriate (e.g., repeated failures).	
Rate limit API and controller access to minimize the harm from automated attack tooling.	
JWT tokens should be invalidated on the server after logout. Developers and QA staff should include functional access control unit and integration tests.	

continued on following page

Table 3. Continued

OWASP recommendations to developer teams	Related Vulnerability
A repeatable hardening process that makes it fast and easy to deploy another environment that is properly locked down. Development, QA, and production environments should all be configured identically, with different credentials used in each environment. This process should be automated to minimize the effort required to set up a new secure environment.	Security Misconfiguration
A minimal platform without any unnecessary features, components, documentation, and samples. Remove or do not install unused features and frameworks.	
A task to review and update the configurations appropriate to all security notes, updates and patches as part of the patch management process (see A9:2017-Using Components with Known Vulnerabilities). In particular, review cloud storage permissions (e.g., S3 bucket permissions).	
A segmented application architecture that provides effective and secure separation between components or tenants, with segmentation, containerization, or cloud security groups (ACLs).	
Sending security directives to clients, e.g., Security Headers.	
An automated process to verify the effectiveness of the configurations and settings in all environments.	
Preventing XSS requires the separation of untrusted data from active browser content. This can be achieved by:	Cross-Site Scripting (XSS)
Using frameworks that automatically escape XSS by design, such as the latest Ruby on Rails, React JS. Learn the limitations of each framework's XSS protection and appropriately handle the use cases which are not covered.	
Escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) will resolve Reflected and Stored XSS vulnerabilities.	
The OWASP Cheat Sheet 'XSS Prevention' has details on the required data escaping techniques.	
Applying context-sensitive encoding when modifying the browser document on the client-side acts against DOM XSS. When this cannot be avoided, similar context-sensitive escaping techniques can be applied to browser APIs as described in the OWASP Cheat Sheet 'DOM based XSS Prevention'.	
Enabling a <u>Content Security Policy (CSP) as a defense-in-depth mitigating control against XSS. It is effective if no other vulnerabilities exist that would allow placing malicious code via local file includes (e.g., path traversal overwrites or vulnerable libraries from permitted content delivery networks).	
Remove unused dependencies, unnecessary features, components, files, and documentation.	Using Components with Known Vulnerabilities
Continuously inventory the versions of both client-side and server-side components (e.g., frameworks, libraries) and their dependencies. Continuously monitor for known vulnerabilities in the components. Use software composition analysis tools to automate the process. Subscribe to email alerts for security vulnerabilities related to components you use.	
Only obtain components from official sources over secure links. Prefer signed packages to reduce the chance of including a modified, malicious component.	
Monitor for libraries and components that are unmaintained or do not create security patches for older versions. If patching is not possible, consider deploying a virtual patch to monitor, detect, or protect against the discovered issue.	
Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.	Insufficient Logging / Monitoring
Ensure that logs are generated in a format that can be easily consumed by a centralized log management solution.	
Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.	
Establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.	
Establish or adopt an incident response and recovery plan, such as NIST 800-61 rev 2 (Cichonski, Millar, Grance, & Scarfone, 2012) or later.	

the International Safe Harbor Privacy Principles in Europe and America, both give formal definitions regarding the security and confidentiality of personal data as well as their anonymization processes.

In a previous section, definitions were given for the direct and indirect identifiers that are included in medical datasets and can be exploited in order to reveal persons' identities. The main techniques used to handle the direct identifiers include either their removal from the database or their replacement with appropriate pseudonyms, depending on the purpose of the dataset (El Emam & Arbuckle, 2013). It is worth noting that, according to the General Data Protection Regulation: "Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.", that is, the pseudonymized data should not be regarded as anonymized, but rather as still personal potentially identifiable information.

Indirect identifiers or quasi-identifiers contain useful information for research and statistical purposes and as a result, are the characteristics to which data anonymization techniques aim. As the security of the data and the usefulness of the information they contain are inversely proportional, the anonymization process should follow a methodical form in order to achieve the best balance between them. The purpose of anonymization is to protect indirect identifiers and sensitive attributes from a reverse attempt to reveal the identity of the data. The techniques and anonymization algorithms are based on some basic models (Eze & Peyton, 2015). The most well-known model is k-anonymity (Samarati & Sweeney, 1998). k-anonymity ensures that every record of a dataset can't be distinguished from at least k-1 other records based on the available indirect identifiers. Therefore, any combination of indirect identifiers should either not appear at all or appear more than once in the dataset. k-anonymity protects from identity recognition, but not from field identifying and sensitive features. Another similar model that has been proposed, mainly to protect demographic components of a database, is k-map (Sweeney, 2001). It considers larger information repositories, which are called population tables and is less restrictive than the k-anonymity model but weaker in terms of security. Three new models (Gionis, Mazza, & Tassa, 2008) have been proposed, called (1, k) -anonymity, (k, 1) -anonymity and (k, k) -anonymity (k, 1) - anonymity, (k, k) -anonymity) that approximate the logic of the k-map model. They provide greater information usefulness but less security than k-anonymity and differ in assumptions about the abilities of the attackers. For the protection of field and sensitive values, the l-diversity model (Machanavajjhala, Kifer, Gehrke, & Venkatasubramanian, 2007) is used to ensure that there are at least l well-represented values for each sensitive feature, where the term well represented is usually defined by a probability threshold: an attacker can't combine his previous knowledge with any sensitive value with a probability of more than $1/l$. There are several versions of this model in the literature, such as distinct l-diversity and recursive (c, l) -diversity (Loukides, Gkoulalas-Divanis, & Malin, 2010). Other models that limit the number of distinct values of sensitive features in an anonymized dataset are (a, k) -anonymity (a, k) -anonymity (Wong, Li, Fu, & Wang, 2006) and k-anonymous p- k-anonymity) (Truta & Vinay, 2006). The t-closeness model (Li, Li, & Venkatasubramania, 2007) is also used to protect against field recognition and sensitive attributes. Accordingly, the distance of the distribution of the values of the sensitive attribute within each equivalence class from the distribution of its values to the total of data must not exceed the upper limit t.

Models have also been created for identity protection while anonymizing diagnostic codes that exist in electronic patient records. The strictest, security-wise, amongst these models, is full k-anonymity (He & Naughton, 2009) that requires at least k records in a publicized database to have the same diagnostic codes, can also be used to anonymize other codes and attributes. Other similar but more flexible models are km-anonymity (Terrovitis, Mamoulis, & Kalnis, 2008) and privacy-constrained anonymity (Loukides et al., 2010). In order to protect the field when the data set contains diagnostic codes, the p-uncertainty model has been proposed, which ensures that the probability that a person is associated with a diagnosis is less than π . Moreover, (h, k, p) -coherence (Cao, Karras, Raïssi, & Tan, 2010) and the PS-rule based anonymity (Loukides, Gkoulalas-Divanis, & Shao, 2013) models have been proposed, which prevent identification and recognition of sensitive features. The d-presence model is the one most commonly used to protect against participation recognition and specifically to ensure that the attacker can't surely know that a person is in the data repository with a probability greater than d. A similar model that does not require data holders to access all of a population's information has also been suggested (Loukides et al., 2010) and is called c-confident d-presence.

All algorithms developed for data anonymization have been based on the models described above. The way in which they process and change the indirect attributes, which is the main stage of anonymization, as well as other elements such as the heuristic strategies they use, is the information on which these algorithms can be compared and classified and finally, emerge as the most appropriate for the anonymization of a health database. (Gkoulalas-Divanis, Loukides, & Sun, 2014) present an analytical summary and classification of algorithms based on the aforementioned models. The most widespread technique used to transform the indirect characteristics of an information repository is generalization (Sweeney, 2002). In generalization, attribute values are replaced by more general ones, without altering their semantics and information they contain. When the attribute has a numerical value, it can be replaced by a range of values that contains the initial value, and if it has a categorical value, a hierarchy of generalization with a tree structure can be followed (for example, the municipality where a person is a resident can become a city or a geographical area when that is not enough, etc.). Applying generalization to all feature appearances is called global recording, while application only to specific occurrences is called local recording (Nergiz & Clifton, 2007). One form of generalization is the micro-aggregation technique (Domingo-Ferrer & Mateo-Sanz, 2002), where the values of a set are replaced with a statistical value (e.g., mean, median). Finally, the technique of suppression is essentially the abstraction of attributes or even of whole records from a set of data. It is the technique used in the direct traits, as mentioned above, but also in the indirect traits that are so rare that they can reveal the identity of certain individuals.

DISCUSSION

Taking advantage of digital health records has the potential to improve drastically clinical care, as well as facilitate data-driven research in many medical fields. However, there is always the risk to rather harm than benefit patients if data security fails to prevent successful attacks, especially given the fact that the prolific integration of technology into medical environments is continuously generating new attack vectors (Seale, McDonald, Glisson, Pardue, & Jacobs, 2018).

Security companies and regulatory authorities are making progress in the effort to tackle the prevalence of cyber-crime, but, at the same time, many healthcare organizations, often simply by delaying to invest in upgrading their systems, thus remaining constantly susceptible to new hacking technologies, are left behind in effectively securing their data, compared to other target industries. For example, (Martin, Martin, Hankin, Darzi, & Kinross, 2017) report that *“many NHS organizations spend as little as 1-2% of their annual budget on IT, compared with 4-10% in other sectors and use many run-on legacy systems that are no longer supported. Indicative of this low level of investment many NHS trusts are still using Windows XP, an operating system that Microsoft stopped supporting in 2014”*. Implementing proper security policies and procedures, is inherently difficult for the healthcare industry, given that it consists of a large number of public and private institutions and lacks the homogeneity and the coordination potential of other sectors (e.g., financial services).

In 2009 Healthcare Information and Management Systems Society (HIMSS) conducted a survey and found that, at the time of the study, despite HIPAA and other initiatives, many of the surveyed healthcare organizations *“do not perform security risk analyses and therefore do not understand their vulnerability to cyber-attack”*, their *“budgets dedicated to security remain low”*, *“still do not have a formally designated Chief Information Security Officer or Chief Security Officer to provide the needed organizational leadership to focus on cybersecurity”*, *“are not using available technologies to secure*

data, such as encryption of computer hard drives”, and “do not have a plan for responding to threats or incidents relating to a security breach” (Harries & Yellowlees, 2013).

Both Private and Public healthcare organizations should increase their efforts to protect themselves, as attacks targeting medical data will continue to increase, mindful of the potential harm to their customers/patients, to their reputation and their financial survivability (a successful breach is estimated to cost, on average, around 3.7 million dollars to clean up (Kruse et al., 2017)). It is therefore imperative that the necessary time and money are invested towards ensuring that healthcare organizations’ software systems are adequately protected, developed, implemented and maintained for the ability to keep sensitive data private and prevent them from falling into the wrong hands.

In order for the new healthcare paradigms to thrive, the public’s trust is imperative. Almost all of the modern medical tools employing personalized care principles and informed evidence-based clinical decisions are based on systems’ interoperability and flexible data access which, in turn, need acceptance, trust, and consent on both personal and social level. Depriving medical practice of these tools due to distrust and fear can render it obsolete. Thus, one could argue that unsuccessful attempts to protect health data have an indirect but significant impact on the quality of the provided healthcare.

REFERENCES

- About The Open Web Application Security Project - OWASP. (2018). Retrieved December 7, 2018, from https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project
- Ali, A., Khan, M., Saddique, M., Pirzada, U., Zohaib, M., Ahmad, I., & Debnath, N. (2016). TOR vs I2P: A comparative study. In *2016 IEEE International Conference on Industrial Technology (ICIT)* (pp. 1748–1751). IEEE. 10.1109/ICIT.2016.7475027
- Amsterdam, J. von. (2018). *Monero versus Bitcoin: The battle of the cryptocurrencies* (vol. 4). Academic Press.
- GDPR Article 83 – General conditions for imposing administrative fines. (2016).
- Astolfi, F., Kroese, J., & Van Oorschot, J. (2015). *I2P - The Invisible Internet Project*. Academic Press.
- Bai, G., Jiang, J., & Flasher, R. (2017). Hospital Risk of Data Breaches. *JAMA Internal Medicine*, 177(6), 878. doi:10.1001/jamainternmed.2017.0336 PMID:28384777
- Bartlett, J. (2015). *The dark net : Inside the digital underworld*. Academic Press.
- Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *The Journal of Electronic Publishing: JEP*, 7(1). doi:10.3998/3336451.0007.104
- Bisson, D. (2015). *5 Social Engineering Attacks to Watch Out For*. Retrieved December 6, 2018, from <https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>
- Boden, E. (2018). *How hackers infiltrate healthcare organizations* | eSentire. Retrieved from <https://www.esentire.com/blog/healthcare-cyber-attack-types/>

Cao, J., Karras, P., Raïssi, C., & Tan, K.-L. (2010). ρ -uncertainty: Inference-proof transaction anonymization. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 3(1–2), 1033–1044. doi:10.14778/1920841.1920971

Center for Internet Security. (2018). *Data Breaches: In the Healthcare Sector*. Retrieved from <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/>

Chideya, F. (2015). *Medical Privacy Under Threat in the Age of Big Data*. Retrieved from <https://theintercept.com/2015/08/06/how-medical-privacy-laws-leave-patient-data-exposed/>

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. doi:10.6028/NIST.SP.800-61r2

Cox, J. (2015). *The Dark Web as You Know It Is a Myth* | WIRED. Retrieved May 31, 2019, from <https://www.wired.com/2015/06/dark-web-know-myth/>

Criddle, L. (2017). *What is Social Engineering? Examples and Prevention Tips*. Retrieved from <https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering>

CWE List Version 3.1. (2017). Retrieved December 7, 2018, from <https://cwe.mitre.org/data/index.html>

Dankar, F. K., & Al Ali, R. (2015). A theoretical multi-level privacy protection framework for biomedical data warehouses. *Procedia Computer Science*, 63, 569–574. doi:10.1016/j.procs.2015.08.386

Data protection in the EU. (2016). European Commission.

Domingo-Ferrer, J., & Mateo-Sanz, J. M. (2002). Practical data-oriented microaggregation for statistical disclosure control. *IEEE Transactions on Knowledge and Data Engineering*, 14(1), 189–201. doi:10.1109/69.979982

Dziembowski, S. (2015). Introduction to Cryptocurrencies. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15* (pp. 1700–1701). New York: ACM Press. 10.1145/2810103.2812704

El Emam, K., & Arbuckle, L. (2013). *Anonymizing health data: case studies and methods to get you started*. O'Reilly Media, Inc.

El Emam, K., Rodgers, S., & Malin, B. (2015). Anonymising and sharing individual patient data. *BMJ (Clinical Research Ed.)*, 350(1), h1139. doi:10.1136/bmj.h1139 PMID:25794882

Emam, K. El. (2013). *Guide to the De-Identification of Personal Health Information*. doi:10.1201/b14764

Eze, B., & Peyton, L. (2015). Systematic Literature Review on the Anonymization of High Dimensional Streaming Datasets for Health Data Sharing. *Procedia Computer Science*, 63, 348–355. doi:10.1016/j.procs.2015.08.353

Garfinkel, S. L. (2016). *Draft (2nd) NIST SP 800-188, De-Identification of Government Datasets*. Academic Press.

Genitsaridi, I., Kondylakis, H., Koumakis, L., Marias, K., & Tsiknakis, M. (2015). Evaluation of personal health record systems through the lenses of EC research projects. *Computers in Biology and Medicine*, 59, 175–185. doi:10.1016/j.combiomed.2013.11.004 PMID:24315661

Gilbert, R., Goldstein, H., & Hemingway, H. (2015). The market in healthcare data. *BMJ : British Medical Journal*, 351, h5897. doi:10.1136/bmj.h5897 PMID:26537618

Gionis, A., Mazza, A., & Tassa, T. (2008). k-Anonymization revisited. In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on* (pp. 744–753). IEEE.

Gkoulalas-Divanis, A., Loukides, G., & Sun, J. (2014). Publishing data from electronic health records while preserving privacy: A survey of algorithms. *Journal of Biomedical Informatics*, 50, 4–19. doi:10.1016/j.jbi.2014.06.002 PMID:24936746

Gold, M., & McLaughlin, C. (2016). Assessing HITECH Implementation and Lessons: 5 Years Later. *The Milbank Quarterly*, 94(3), 654–687. doi:10.1111/1468-0009.12214 PMID:27620687

Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to Information Security—Public Health Implications. *The New England Journal of Medicine*, 377(8), 707–709. doi:10.1056/NEJMp1707212 PMID:28700269

Grassi, P. A., Fenton, J. L., Newton, E. M., Perln, R. A., Regenscheid, A. R., Burr, W. E., ... Theofanos, M. F. (2017). *Digital identity guidelines: authentication and lifecycle management*. doi:10.6028/NIST.SP.800-63b

Guzek, M., Bouvry, P., & Talbi, E.-G. (2015). A Survey of Evolutionary Computation for Resource Management of Processing in Cloud Computing [Review Article]. *IEEE Computational Intelligence Magazine*, 10(2), 53–67. doi:10.1109/MCI.2015.2405351

Harries, D., & Yellowlees, P. M. (2013). Cyberterrorism: Is the U.S. Healthcare System Safe? *Telemedicine Journal and e-Health*, 19(1), 61–66. doi:10.1089/tmj.2012.0022 PMID:23113795

He, Y., & Naughton, J. F. (2009). Anonymization of set-valued data via top-down, local generalization. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 2(1), 934–945. doi:10.14778/1687627.1687733

Hern, A. (2018). *What is GDPR and how will it affect you?* | Technology | The Guardian. Retrieved from <https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you>

HIPAA. (2018). *When Was HIPAA Enacted? HIPAA (Health Insurance Portability and Accountability Act)* | *whatis.com*. (2017). Retrieved from <https://searchhealthit.techtarget.com/definition/HIPAA>

HIPAA Privacy Rule and Its Impacts on Research. (2005). Retrieved from <https://privacyruleandresearch.nih.gov/healthservicesprivacy.asp>

Hurlburt, G. (2017). Shining Light on the Dark Web. *Computer*, 50(4), 100–105. doi:10.1109/MC.2017.110 PMID:29213147

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75–87. doi:10.1016/j.chb.2016.09.012

Koczkodaj, W. W., Mazurek, M., Strzałka, D., Wolny-Dominiak, A., & Woodbury-Smith, M. (2018). Electronic Health Record Breaches as Social Indicators. *Social Indicators Research*. doi:10.1007/11205-018-1837-z

Koyun, A., & Al Janabi, E. (2017). *Social Engineering Attacks. Journal of Multidisciplinary Engineering Science and Technology* (Vol. 4). JMEST.

Kruse, C. S., Frederick, B., Jacobson, T., & Kyle, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. doi:10.3233/THC-161263 PMID:27689562

Li, N., Li, T., & Venkatasubramania, S. (2007). t-Closeness : Privacy Beyond k-Anonymity and -Diversity. *IEEE 23rd International Conference*, (3), 106–115. 10.1109/ICDE.2007.367856

Lord, N. (2018a). *Top 10 Biggest Healthcare Data Breaches of All Time* | *Digital Guardian*. Retrieved from <https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time>

Lord, N. (2018b). *What is GDPR (General Data Protection Regulation)? Understanding and Complying with GDPR Data Protection Requirements* | *Digital Guardian*. Retrieved from <https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection>

Loukides, G., Gkoulalas-Divanis, A., & Malin, B. (2010). Anonymization of electronic medical records for validating genome-wide association studies. *Proceedings of the National Academy of Sciences of the United States of America*, 107(17), 7898–7903. doi:10.1073/pnas.0911686107 PMID:20385806

Loukides, G., Gkoulalas-Divanis, A., & Shao, J. (2013). Efficient and flexible anonymization of transaction data. *Knowledge and Information Systems*, 36(1), 153–210. doi:10.1007/10115-012-0544-3

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity. *ACM Transactions on Knowledge Discovery from Data*, 1(1), 3. doi:10.1145/1217299.1217302

Martens, B., & Teuteberg, F. (2012). Decision-making in cloud computing environments: A cost and risk based approach. *Information Systems Frontiers*, 14(4), 871–893. doi:10.1007/10796-011-9317-x

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Clinical Research Ed.)*, j3179. doi:10.1136/bmj.j3179 PMID:28684400

Mell, P. M., & Grance, T. (2011). *The NIST definition of cloud computing*. doi:10.6028/NIST.SP.800-145

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic cash system. *Bitcoin*, 9. doi:10.1007/10838-008-9062-0

Nergiz, M. E., & Clifton, C. (2007). Thoughts on k-anonymization. *Data & Knowledge Engineering*, 63(3), 622–645. doi:10.1016/j.datak.2007.03.009

Noether, S., Mackenzie, A., & Research Lab, T. M. (2016). Ring Confidential Transactions. *Ledger*, 1, 1–18. doi:10.5195/LEDGER.2016.34

Olavsrud, T. (2010). *9 Best Defenses Against Social Engineering Attacks*. Retrieved December 6, 2018, from <https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm>

Orito, Y., & Murata, K. (2005). Privacy protection in Japan: cultural influence on the universal value. *Electronic Proceedings of Ethicomp*, 5.

Pulkkis, G., Karlsson, J., Westerlund, M., & Tana, J. (2017). Secure and Reliable Internet of Things Systems for Healthcare. In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 169–176). IEEE. 10.1109/FiCloud.2017.50

Samarati, P., & Sweeney, L. (1998). Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement Through Generalization and Suppression. *Proceedings of the IEEE Symposium on Research in Security and Privacy*, 384–393. 10.1145/1150402.1150499

Seale, K., McDonald, J., Glisson, W., Pardue, H., & Jacobs, M. (2018). MedDevRisk: Risk Analysis Methodology for Networked Medical Devices. *Hawaii International Conference on System Sciences 2018 (HICSS-51)*. 10.24251/HICSS.2018.414

Singhealth, T., Attack, C., Author, C. O. I. F., Jayakumar, S., Attack, S. C., Findings, C. O. I., ... Url, C. D. (2019). *This document is downloaded from DR-NTU, Nanyang Technological SingHealth Cyber Attack : Learning from COI Findings*. Academic Press.

Spitzer, J. (2018). *Healthcare data breaches spike significantly in 7 years: 5 things to know*. Retrieved from <https://www.beckershospitalreview.com/cybersecurity/healthcare-data-breaches-spike-significantly-in-7-years-5-things-to-know.html>

Summary of the HIPAA Security Rule | HHS.gov. (2013). Retrieved from <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

Sweeney, L. (2001). *Computational disclosure control: a primer on data privacy protection*. Massachusetts Institute of Technology.

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 10(05), 571–588. doi:10.1142/S021848850200165X

Terrovitis, M., Mamoulis, N., & Kalnis, P. (2008). Privacy-preserving anonymization of set-valued data. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 1(1), 115–125. doi:10.14778/1453856.1453874

Top 10-2017 Details About Risk Factors - OWASP. (2017). Retrieved December 6, 2018, from https://www.owasp.org/index.php/Top_10-2017_Details_About_Risk_Factors

Truta, T. M., & Vinay, B. (2006). Privacy protection: p-sensitive k-anonymity property. In Null (p. 94). IEEE.

Washington, V., DeSalvo, K., Mostashari, F., & Blumenthal, D. (2017). The HITECH Era and the Path Forward. *The New England Journal of Medicine*, 377(10), 904–906. doi:10.1056/NEJMp1703370 PMID:28877013

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict and Terrorism*, 39(3), 195–206. doi:10.1080/1057610X.2015.1119546

What is the HITECH ACT? | What HITECH Compliance Means. (2009). Retrieved from <https://compliance-group.com/what-is-the-hitech-act/>

Withrow, S. C. (2010). How to avoid a HIPAA horror story: The HITECH Act has expanded the financial risk for hospitals that do not meet the privacy and security requirements under HIPAA. *Healthcare Financial Management*, 64(8), 82–89. PMID:20707266

Wong, R. C.-W., Li, J., Fu, A. W.-C., & Wang, K. (2006). (α , k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 754–759). ACM.

KEY TERMS AND DEFINITIONS

Anonymity: Anonymity and thus anonymous data is any information from which the person to whom the data relates cannot be identified, whether by the company processing the data or by any other person.

Cloud Computing: Cloud computing is a type of computing that relies on shared computing resources rather than having local servers or personal devices to handle applications.

Cyberattack: A deliberate exploitation of computer systems, technology-dependent enterprises and networks.

GDPR: General Data Protection Regulation is a new set of rules governing the privacy and security of personal data laid down by the European Commission.

Private Health Data: Is defined as individually-identifiable health data, which is exquisitely sensitive. Being linked to an individual, the private health data can only be shared with the permission of the individual.

The Emerging Threats of Web Scrapping to Web Applications Security and Their Defense Mechanism

Rizwan Ur Rahman

Maulana Azad National Institute of Technology, Bhopal, India

Danish Wadhwa

JayPee University of Information Technology, Solan, India

Aakash Bali

JayPee University of Information Technology, Solan, India

Deepak Singh Tomar

Maulana Azad National Institute of Technology, Bhopal, India

INTRODUCTION

Nowadays the Internet is at its peak everything is available online or is going to be available soon. So the Internet has provided us with some facilities like online Shopping, Bookings of trains and buses tickets, education and many more. However, there is always another side to the coin, with the facilities comes the cyber attacks of various types like DDOS, Man in the Middle, SQL Injection etc. One of them is Web scraping which is a very serious issue nowadays it's affecting the market of online e-commerce at very great extent.

It is an ongoing threat that aims to take sensitive data from a victim or from web applications. According to the Automated Threat Handbook for Web Applications published by the Open Web Application Security Project, web scraping is exploited at companies in industries including education, financial institutions, government agencies, hospitals, and retail (Munzert et al., 2014).

The main objective of this chapter is to scrutinize to what degree web scraping can cause a threat to web application Security. In first section the terms in the chapter are defined, and an adequate overview of web scraping in context to web application security is presented in order to provide the reader with an understanding of the background for the remaining sections.

The next section examines the classification of web scraping such as content scraping, web scraping, price scraping, data aggregation, database scraping in general and reviews the most widely used scraping tools such as Visual Web Ripper, Web Content Extractor, Mozanda Web Scraper and Screen Scraper.

A section dedicated to Defense Mechanism including detective and preventive mechanisms are presented. Subsequently, the aim of this chapter is to provide review of vulnerabilities, threats of web scraping associated with web application applications and effective measures to counter them.

WEB SCRAPING

Web scraping is also known by some other names like web harvesting and web data extraction basically is used for extraction of data from the websites on the WORLD WIDE WEB. In other words, it can be defined as the process consisting of the extraction and combination of content gathered from the web in a systematic manner (Vargiu & Urru, 2012).

Software applications are available for doing the web scrapping which may do their work of accessing the World Wide Web using Hypertext Transfer Protocol or web browser. Web scraping can also be done manually by the user but is preferably done in an automated fashion implemented using a bot or web crawler. In this, some software also known as web robot is mimicking the browsing between the web and the human in a conventional web traversal.

This robot may gather the data from as many websites as needed and the parsing of the contents is done to easily find and fetch the data required and stores them in the structures as desired.

Generally, this task of web scraping is somewhat similar to copying; in this particular data is collected and copied from the Internet into some manageable and readable storage structure like some spreadsheets or databases.

In this process, the web page is downloaded or fetched (it happens whenever the browser opens up some pages) first and saved for later use and then the data is extracted from it. Hence we can say that web crawling is an important component of the process.

At the second step of the process the content present in the page is parsed, searched or some type of reformatting is done to understand the content for the data to get it inserted into the spreadsheets or database by copying. Generally, the web scrapping software may sometime take a part of the page which can be useful for the authority for some other purpose.

Web Scrapping is being used in various things in today's life like in advertisements and marketing generally by contact scraping and also an important part of the application made for data mining and web mining, and sometimes used to do some price comparisons, for online price change monitoring, weather data monitoring, research and for providing a service to the user where the content comprises of more than one source also known as web mashup for instance, like trivago and mybestprice applications.

Basically, these web scrapers are APIs which are used to extract data from a web page or a website present on the Internet. Also, some big companies like Amazon Web Services and Google provide web scrapping tools free of cost to end users.

Nowadays a new form has been also used for web scrapping which consists of listening or monitoring the data feed from the web servers. And also some web scraping systems are also using DOM parsing techniques, computer vision and NLP to simulate human browsing as to pass the checks for bots that some websites are using to prevent web scrapping.

Types Web Scrapping

There are various types of web scraping. This section explores the categories of widely used web scraping techniques. These are Data Scraping, Content Scraping, Price Scraping, Database Scraping, News Scraping, Article Scraping and Email Harvesting

Data Scraping

It is a process in which computer program gathers data from some humanly understandable output that is coming from another computer program. Generally, data transfer between programs is done using various data structures best for processing by computers, not humans. These interchangeable formats and protocols are rigid in structure, mostly well documented and easy to parse.

The main difference between data scraping and parsing is just that it scrapes the data which was for display for humans and was not used as input to another program. It ignores data in binary format. It is mostly used as an output to a legacy system which has no other way by which it can display the data or it is used for the systems for which the APIs are not good enough to provide the data. It is not the most preferable technique to be used to extract the data; it is usually the last option when no other technique is available (Yang et al., 2010).

Content Scraping

It is generally the technique of lifting off the displayed content from various websites and using it somewhere else or displaying it on other website. The technique is illegal as it is generally done without the permission of the original source. The content scrapers mostly copy the whole content being displayed and share it as their own content. It is an illegal method to steal the content from a trusted website and publishing to another website without the knowledge of the content's owner (Cormode & Krishnamurthy, 2012).

Content scraping is being done at the expense of the website that has invested time, resources and money as it will also affect their SEO ranking. It can be done by manually copying and pasting or by using special software or by HTTP programming etc.

Price Scraping

The technique of extracting or collecting the prices of various sellable things available over the internet on various websites without the consent of the corresponding authorities and slowing down their network by frequently requesting for the data being displayed by them. It is generally used to beat the competition in the market or to make profits out someone's loss by planning according to the scrapped data and lowering the prices of things being searched by users to attract them to their own website and increase their profits through ads being shown on the website (Rahman & Tomar, 2018).

Price scraping can be done for various uses in order to predict some share of the market being occupied by the biggie of e-commerce or for the newcomers to know about the various new trends being prevailed in the market in order to enter the competition of selling things online and also to gather the information about the supply and demand of various products being sold on the website.

It's illegal to scrape the data for commercial use but still, it is being done by many companies for various purposes and there are no efficient methods present to have a check on it (Parikh et al., 2018).

Database Scraping

The technique of directly extracting data from the database is known as the Database scraping. Sometimes the data is being stored in the database file or .csv file in which the data is being stored in the structured format for some special use or classification to do some calculation etc.

The data is being stored in columns and rows so there may not be difficulty in scraping the data as the data has some pattern that is stored. It can be used for various purposes but is basically used for research purposes as a large database are being scraped off data to classify the data into some important information which can help in predicting the results of some work or to provide automation.

Sometimes it is also used for commercial purposes in order to scrape the database of persons personal details without his/her consent. So it can be used for illegal as legal purposes (Mitchell, 2018).

News Scraping

The techniques of scraping used for scraping the news from the newspapers websites is known as news Scraping. The articles of news are being scraped to some blogs or some database in order to do some discussion or to have the database of the news which can be used to predict the type of acts of crimes can happen or to calculate the results of the distribution of the crimes happening.

It can be used by some educational purposes in order to be updated on the various things happening or we can say enhance student's general knowledge in preparation of various exams. It generally doesn't affect much but it lowers the ranking of the website SEO rankings and the Web ratings and the traffic on the website will be affected accordingly (Pak, 2017).

Article Scraping

The scraping of the data being written over blogs or various websites on the internet is known as Article scraping. Generally done for the purpose if the collection of data that can be used for various purposes like educational, research etc.

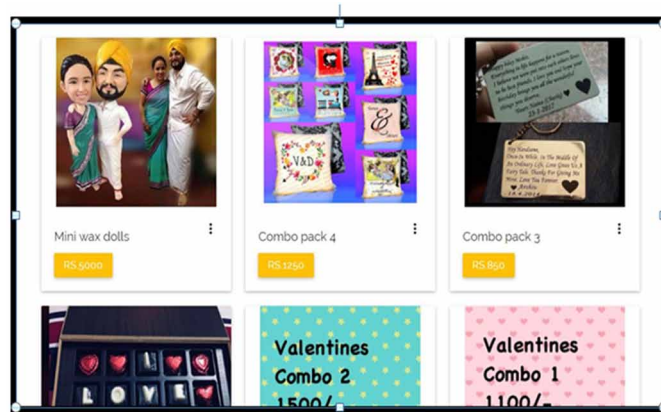
This practice can be used for some type of security purposes sometimes in order to find some potential threats to the nation or some specific words being used against some things of political importance or It can be used to ease the process of collecting data on some specific topic which is new and evolving and to improve the related information on that specific topic in order to provide reliable information which can be used further for various process developments and experiments (Ou-Yang, 2013).

Email Harvesting

The mechanism to obtain a large number of email addresses using different methods or techniques. The main purpose of email harvesting is for spamming or advertising purpose.

It is mostly done by some specialized harvesting software or programs also known as the harvester. The email can be scraped using various ways like from mailing lists, stored data of a web browser, from yellow pages through social engineering etc. Some spammer use the dictionary attack to extract an email address, in this the valid emails addresses are found by means of guessing the most used usernames .or by offering a product or service to users absolutely free till they provide their genuine email address and then from them collect email addresses for spamming or bulk email (Polakis et al., 2010).

Figure 1 .The products page of an e-commerce website



AUTOMATED WEB SCRAPING TECHNIQUES

Text Pattern Matching

It is a method of doing the extraction of data from the parsed web page in the process of web scraping by using the Regular Expression matching in the collected data.

Regular Expression can be defined as a sequence of characters that define a search pattern. Generally, this can be used by various algorithms of string searching to be used on strings and for validating some inputs taken by the user (Usmanov, 2017).

A regex processor is the breaks down the regular expression into an internal representation which is executed and matched for a string that represents the text that is searched in. An easy way to specify a finite set of strings is to list its members. For example

There is a set containing two strings “Handel”, “Haendel” can be matched by the pattern **H(alae?)ndel;**

The regular expression is widely used in UNIX. There is a module represent in python which provides full support for PERL-like regexes. The whole process of doing web scraping can or can't have a regex in your implementation of the scraper. It depends on the type of website being scraped and is the last resort to do the scraping when no other methods can be used in order to scrape the useful data from the website. It is generally used when there is no pattern defined in a website or the data is randomly given and there is only some textual pattern present in the website.

For example in Figure 1, the products page of an e-commerce website is shown and in Figure 2 its corresponding HTML code

For this particular website having price as a text on the buttons of the products along with the Symbol “Rs.”. To scrap or extract the price of product from this webpage following script is executed in python shown in figure 3.The snapshot of the outcome is shown in figure 4.

HTML Parsing

As we know every website present on the internet are written using HTML (Hypertext Mark-up Language).As it is a structured language so that implies that every web page is a structured document. And sometimes we might need data from the websites and web pages and preserve their structure as well.

Figure 2. HTML code of products page of an e-commerce website

```

<div class="card">
<div class="card-image waves-effect waves-block waves-light">
<a href="product.php?pid=EG0051"></a>
</div>
<div class="card-content">
<span class="card-title activator grey-text text-darken-4">Mini wax dolls<i class="material-icons right">more_vert</i></span>
<p><a href="product.php?pid=EG0051" class="btn amber waves-light btn">Rs.5000</a>
</p>
</div>
<div class="card-reveal">
<span class="card-title grey-text text-darken-4">EG0051<span class="pnmsize">(Mini wax dolls)</span><i class="material-icons right">close</i></span>
<p>Wax miniatures- can be done for any picture.</p>
<a href="product.php?pid=EG0051" class="btn btn-large amber waves-light btn" style="font-size:22px; font-weight: bold;
<i class="material-icons left">shopping_cart</i>Rs.5000</a>
</div>
</div>
</div>

```

Figure 3. Python script for price scrapping from products page of an e-commerce website

```

# import libraries

import bs4
import requests
import re

res = requests.get("http://<examplewebsitename>/")
soup = bs4.BeautifulSoup(res.text, 'html.parser')

print(re.findall(r'Rs\.[0-9]+\.', res.text))

```

Figure 4. The snapshot of the outcome of Python script for price scrapping

```

['Rs.5000', 'Rs.5000', 'Rs.1250', 'Rs.1250', 'Rs.850', 'Rs.850', 'Rs.600',
'Rs.600', 'Rs.1500', 'Rs.1500', 'Rs.1100', 'Rs.1100', 'Rs.2000', 'Rs.2000',
'Rs.1200', 'Rs.1200', 'Rs.450', 'Rs.450', 'Rs.1399', 'Rs.1399', 'Rs.2000',
'Rs.2000', 'Rs.450', 'Rs.450']

[Done] exited with code=0 in 1.951 seconds

```

In general, parsing is basically to break (a sentence) into its components and specify their syntactic roles. Parsing or syntactic analysis is the process of analyzing a collection or string of symbols can be in the natural language or in a computer language agreeing to the rules of a formal grammar.

In this case of HTML parsing comprise of:

Taking in HTML code and extracting needed information like the title of the page, paragraphs in the page, headings in the page, links etc.

The request will be made to get the web page using request module get function and then the extracted HTML script will be converted into HTML tree which will have the structured data from that we will make use the various ways to go over that tree like XPath or CSSSelect and then the extracted t=data will be added to the various lists.

The lxml is a pretty extensive library written for parsing XML and HTML documents in no time and can also handle messed up tags in the process of parsing.

There are two ways to extract the data from the web page after being converted into HTML tree by using XPath or CSSSelect. This example will make the use of XPath. XPath is a way of locating information in various structured documents like HTML and XML.

DOM PARSING

As we have explained parsing in the previous techniques. There are two types of parsers present

Top-Down Parser

Top-down parsing can be seen as a dry run to find the left-most derivations of an input stream by looking for parse trees using a top-down opening out of the given approved set of grammar rules. Tokens are generally put to use from left to right.

Bottom-Up Parser

A parser can begin with the input and tryout to rework it to the start symbol. The parser attempts to detect the most primary elements than the elements comprising of these and so on.

DOM stands for the Document Object Model is a programming API for HTML and XML documents or web pages. It specifies the logical structure as well as the way to access the document and manipulate it.

With DOM developers can create and build documents, navigate through their structure and can add, modify or delete content or elements.

In Document Object Model, documents consist of a tree-like logical structure or a forest comprising of more than one tree. In this, the documents are modeled using objects and the model contains not only the structure of the document but also the behavior of a document and the objects which it comprises of.

While scraping a website the first step is to request the web page and receive the page HTML DOM tree. After this, the step is to parse the DOM tree to extract the data we want. Usually, it is done with string operations and using regular expressions. The other methods are by using DOM parser library either CSSSelect or XPath to extract the DOM elements which contain the required information.

Optical Character Recognition (OCR) Techniques

Optical Character Recognition techniques can be used for images or documents which cannot be parsed into text directly which contain some information required.

It is the mechanical or electronic conversion of images of typed handwritten or printed text into machine-encoded text. It is widely used for solving CAPTCHA's (Completely Automated Public Turing test to tell Computers and Humans Apart)

Which is used as the preventive measure for the web scraping done on the web pages on various websites. The OCR technique is useful in some web pages where the required information is in some images or PDFs so to scrape that required information this technique is used. It is not much efficient but is constantly worked upon to increase its efficiency to help in scraping and various other streams (Cheng & Evans, 2012).

There are four types of Character Recognition Techniques:

1. **Optical Character Recognition (OCR):** Generally targets typewritten text, one glyph (an elemental symbol within an agreed set of symbols, intended to represent a readable character for the purposes of writing) or character at a time.
2. **Optical Word Recognition:** Targets one word at a time (generally for languages use a “ ” as a word splitter)
3. **Intelligent Character Recognition (ICR):** Targets handwritten print scripts or cursive text one glyph or character at a time using Machine Learning.
4. **Intelligent Word Recognition:** Targets one word at a time. Mostly used for languages where glyphs are not separated in cursive script.

LEGALITY OF WEB SCRAPING

The legality of web scraping depends upon the type of data you are scraping from the website and how you use it. For ex:- the hotel booking app like Trivago scrape the prices from all the other hotel booking website and compare it only so it is legal but if it scrape the data and show its prices less than other sites in order to increase its own customer base then it become illegal.

In general if the information scraped is available to public is used in friendly way it is legal. Site like LinkedIn sue the people who try to scrape their site without permission and reasons are:-

1. Breach of Contract
2. Misappropriation
3. Trespass
4. Violation of Computer Fraud and Abuse Act

So to not get in trouble while scraping data from any website one should try to follow these advices:

1. Respect the Terms of Service
2. Obey the rules of Robot.txt
3. Use an API instead of scraping data
4. User Agent field must be filled with right information
5. Do not try to publish your scraped data on public platform until you have the permission to do so.

WEB SCRAPING TOOLS

Scraping of data from any website in large extent is very hectic task and consume a lot your time. So, it can be done with the help of various tools which helps us to extract the information from web very easily. These tools can be used to compare prices of products, scrape user profiles from various social network sites, monitor the real estate prices etc. There are various tools present in the market which are used to scrape the data from websites. For example:-

1. Visual Web Ripper
2. Web Content Extractor
3. Mozenda Web Scraper
4. UI Path-Robotic Process Automation
5. OutWit Hub
6. Screen Scraper
7. WebHarvy
8. Easy Web Extract
9. Scrapy
10. Import io

Visual Web Ripper

Visual web ripper is the powerful visual tools used to scrape the data from any website automatically. It walk through the whole website and collects the needed the data like product catalog, search information etc. Also it saves the data in structured form in spreadsheets as CSV or XML file. It runs on the scheduled basis so the data extracted remains up to date. It is very easy to use as you can extract the data by just clicking on the data element. Anyone having good .NET programming skills can easily use this tool into their own application (Haddaway, 2015). The features of this tool are mentioned below:-

- It extracts the whole data and saves it in structured form.
- Very user friendly.
- Harvests data undetected.
- Command line processing and comprehensive API.

Web Content Extractor

Web Content Extractor can be used if anyone wants to extract typical data from multiple web pages. It is designed to increase the productivity as well as the effectiveness of data scraping. It does not require and coding but it provides point and click web interface.

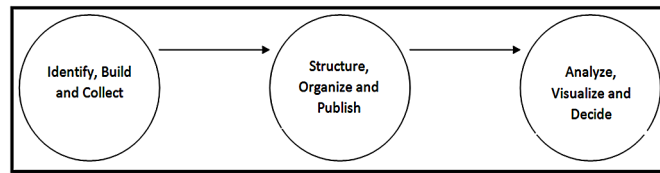
Web Content Extractor allows a user to scrape the data even from the cloud. It is accessible from any web browser on any operating system (Herrouz et al., 2013). Some of the features of Web Content Extractor are mentioned below:-

- Reliable and powerful extracting tool
- User can configure to work on specific links and it helps in accurate web scraping.
- User just has to specify the data extraction process which can be done by few clicks and from that the extractor will do the rest of the work.

Mozenda Web Extractor

The following approach is followed by this software to extract the information (Agrawal & Agrawal, 2013). The Working of Mozenda Web Extractor is shown in Figure 5.

Figure 5. Working of Mozenda web extractor



- **Identify, Build and Collect:** Extract files, images, text and PDF content from the web pages and transform them into the structured form.
- **Structure, Organize and Publish:** Organize and prepare the data files for publishing. User can transport information directly in CSV, XML and JSON files.
- **Analyze, Visualize and Decide:** Collect and publish your web data to your preferred BI Tool or database.

UI Path- Robotic Path Automation

Robotic Path Automation is the technology with the help of which anyone can configure the computer software. Also it can be described as robot working in the form of human in order to execute some business process. To capture the data and manipulate it the RPA robots uses the user interface. RPA robots never sleeps and makes no mistake.

Works that can be performed using RPA robots are:

1. Log into an application
2. Connect to system API
3. Copy and paste data
4. Move files and folders
5. Extract and process structured and semistructured content from documents, PDFs, emails and forms.
6. Read and write to database
7. Scrape data from web
8. Make calculations

Various features of RPA are:-

- Fast implementation
- Reduce the manual effort
- Improve customer service

OutWit Hub

OutWit Hub breaks down the content of webpage into different constituents so that it can navigate through the different pages automatically, extracts data and organize the extracted data into the usable collection.

This tool can be accessed by anyone whether a person wants to scrape the specific data or just a particular document, image etc. A person without any programming knowledge can see the extracted data easily. Extracted data can be transported to CSV, Excel Spreadsheets, HTML files etc. and are directly saved onto the user's hard disk. The latest version of this software is 7.0.0.56 and is available for free download.

Screen Scraper

Screen scrapping is a process in which data from one screen of any application is scraped and shown on the display of another application (Holmberg et al., 2015).

Screen scraper provides the web scraping services. Firstly you have to decide what to scrape from the web i.e. Text, images, data etc. then user chooses the type of file extension in which he/she wants the data to be organized and then screen scraper will do the rest of the work for you.

WebHarvy

WebHarvy is software which is used to scrape the data. It has various features (Johnson & Gupta, 2012):

1. **Easy Data Selection:** Similar to Web Content Extractor it has point and click interface which makes it easy to use. No code or scripts are required to scrape data.
2. **Intelligent Pattern Detection:** If data repeats itself like names, address, phone number etc. There is no need to configure the software but it automatically detects the pattern and scrape the data for you.
3. **Save to file and database:** Similar to other softwares you can save the scraped data in any form of file like Excel, CSV, XML etc.
4. **Crawl Multiple Pages:** If any of the data is displayed in multiple pages then you can easily extract data with the help of WebHarvy. You have to provide the link of the next page and then WebHarvy can extract data easily.
5. **Safeguard Privacy:** Sometimes web scraper softwares get blocked due privacy issues in some sites. To prevent this problem WebHarvy uses the proxy server so that it can scrape data without any hindrance.
6. **Regular Expression:** A user can apply regular expression on text or HTML source and scrape the matching data. This feature provides the flexibility to user while scraping data.

Easy Web Extract

Easy Web Extract works in three steps (Abburu & Babu, 2013):

1. **Web Data Pattern Specifying:** In this phase the user tells the software what data to scrape and from where.
2. **Automate Scraping Web Data:** After the step-1 software will automatically find proper urls and extract information based on the data pattern.
3. **Export Scraped Data:** The scraped data is stored in to the files which can be of various extensions.

Scrapy

Scrapy is an open source and collaborative framework which is used to extract the data from a website. It requires web crawlers to be designed by user and run it over any website to scrape the data (Myers & McGuffee, 2015).

Example of code which scrape the quotes from a website <http://quotes.toscrape.com>.

```
import scrapy
class QuotesSpider(scrapy.Spider):
    name = "quotes"
    start_urls = [
        'http://quotes.toscrape.com/tag/humor/',
    ]
    def parse(self, response):
        for quote in response.css('div.quote'):
            yield {
                'text': quote.css('span.text::text').extract_first(),
                'author': quote.xpath('span/small/text()').extract_first(),
            }
        next_page = response.css('li.next a::attr("href")').extract_first()
        if next_page is not None:
            yield response.follow(next_page, self.parse)
```

Put the above code in file named quotes_spyder.py and run the spider using runspider command:

```
scrapy runspider quotes_spyder.py -o quotes.json
```

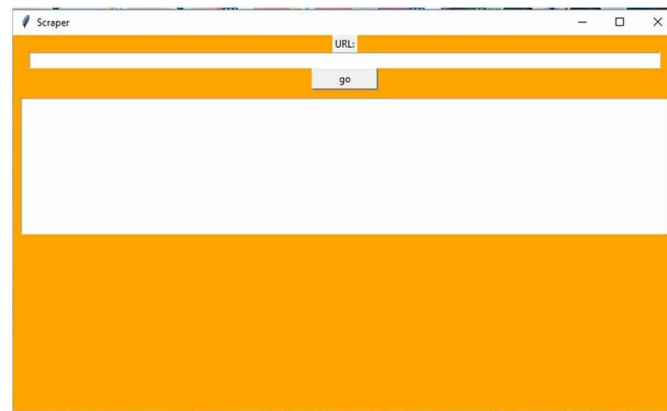
When the above command finishes you will get quotes.json file which will consist of scraped quoted from the above mentioned website.

ImportIO

ImportIO is the company which develops the data extraction or scrapping software. Its data extraction technique is machine learning based and no coding is required to extract data (Mitchell, 2013).

Features of ImportIO extractor are:-

Figure 6. Snapshot of browser window for price scrapping



1. Point and click training
2. Machine Learning Auto suggestion
3. Get data from behind login
4. Webhooks (where you want to store data)
5. Extract data from multiple pages
6. Auto optimized Extractors
7. Control via API or UI
8. Extractor Tagging

Attack Scenario of Price scrapping

The system which we have developed mimics the actual scenario in which the scraper attacks any website and what mechanism can be used to detect the presence of the bot on the website. The System comprises two Subsystems:

Attack System

The attacking scenario contains many steps on the type of scraping is done. Here to do the price scraping we have to build the scraper in three parts

1. GUI Graphical User Interface
2. Web Crawler or Spider
3. Web Scraper

Graphical User Interface

The GUI refers to some type of visible program output, with which the user can interact to give the input to the scraper to do price scrapping. In this, we have used the libraryTkinter in python 3. In this, we have made a simple Browser window consisting of one input field which takes the input from the user of the website to be scraped off the price and then there is a button named label “go” is present which

Figure 7. Working of spider

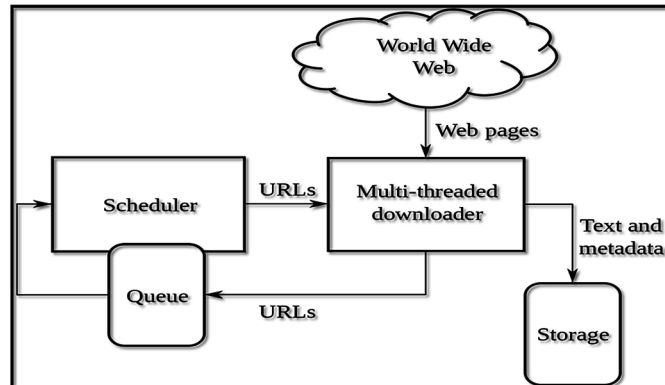
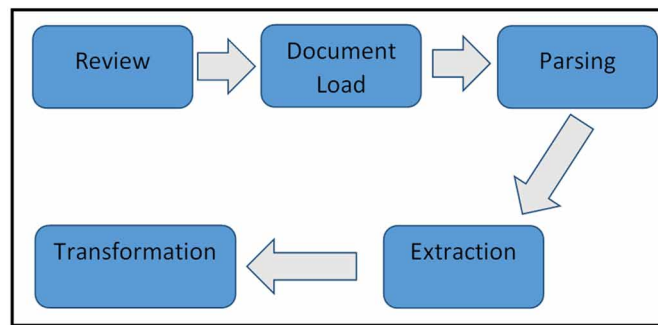


Figure 8. Working of web scraper



starts the spider and sends the URL of the website to the spider. The snapshot of Browser Window for Price Scrapping is shown in Figure 6

Spider or Web Crawler

In this spider, the basic work that is done is to collect all the links present on the websites that belong to the website only. The process of crawling the entire website is a very complex process as nowadays we know that the single website contains a great number of links present in it or have a very high amount of pages present in the website. So we have to make a web crawler which is efficient and speedy too that increases the difficulty of the making of spider very much.

So to overcome this problem, we have to divide the work into different workers or spiders. This can be done by using threads in the making of spider which can divide the work in them and can specify the work. This is an efficient process to specify the process but it creates one more problem of inconsistency and redundancy as well as various Spider will try to access the same link and will do the scraping or crawling of the web pages multiple time which is a waste of resources and time as well. So there is one solution to this problem that we are facing that if we can make only one instance of the links queued and one instance of links to be crawled so that every spider knows which link to pick out of the queued ones. When the process of the spider comes to an end the process of the scraping begins. All those crawled

links of the website are stored in some temporary memory or in a file which can be accessed by the scrapper after the crawling is being done. Figure 7 shows the working of spider.

Web Scraper

The scraper takes the input of the links which has been crawled by the spider and starts the scraping of data in the following ways. The overall working of Web Scraper is shown in Figure 8.

Step1: Review

It is the most important step of the web scraping as all of the further process depends on this step. Because it is the step in which the structure of the web page is analyzed and the most effective techniques of scraping are decided as to how to scrape the data or in which way we can filter out the data from the web page.

Step 2: Access or Document Load

In this step, the page is requested from the server and the page downloaded from the internet in order to parse it into a string of characters. Then there comes the HTML parser which converts the downloaded page into Document Object Model so the scraper can scrape out the data from the structured document easily by accessing various techniques HTML tags and Dom objects.

The requests library can be used to and the get method:

```
from requests import get  
response=get(url)
```

Step 3: Parsing

Once the page is parsed into the required document or data then it is analyzed for any type of pattern present in the document where the required data is being stored in the document as finding some pattern will ease the process of filtering the information out of the data or the document.

The libraries it can make use of are BeautifulSoup and HTML Parser

```
import bs4  
soup = bs4.BeautifulSoup(response.text, 'html.parser')
```

Step 4: Extraction

Then there comes the process of filtering the data out or scraping as we know there are various steps of filtering the data is through Regular expression, accessing the DOM object or by accessing the Html tags etc. But it depends on the placement of the data inside the HTML page just loaded on to the buffer. So different methods are applied to filter out the data sometime the methods are combined to do the scraping.

```

req = requests.get('http://<examplewebsitename>/')
soup = bs4.BeautifulSoup(req.text, 'HTML.parser')
elements = soup.find_all('div', {'class': 'card-content'})
record = []
for element in elements:
    name = element.span.contents[0]
    price = element.p.a.text
    price = price[price.find('Rs.')+3:-1]
    pid = element.p.a['href']
    start = pid.find('pid')+4
    prodId = pid[start:-1]
    record.append((prodId, name, price))

```

Step 5: Transformation

After the data is filtered out the structured or meaningful information is present on hand which has to be stored somewhere in order to use that information in near future. So the data can be stored in various places like in CSV files, database, cloud and many more. the data is stored in forms of tables mostly as it is easier to classify that data for further use in various things.

The pandas module can be used to store the DataFrame of the data:

```

import pandas
import os
records.append((ip, date, method, byte, name))
df = pandas.DataFrame(
records, columns=['ip', 'date', 'method', 'byte', 'name'])
df.to_csv('logdata.csv', index=False, encoding='utf-8')

```

This is the whole process of scraping the data off the website we are generally taking the case of price. So the main websites will be consisting of the various e-commerce website present on the internet. There are thousands of e-commerce websites present on the internet which can be scraped for their data. This data can be used to enhance one's business by getting the lowest price for the things being searched or posted on his/her website. And increasing the hits on the website and also increasing the customer market and the profit by selling these things on the fewer prices than the competitor websites.

DEFENCE MECHANISM

Scraping is very useful when we want to scrape large amount of data from any website as it saves our time and resources but sometimes people make the wrong use of this technique. For instance, we have two online e-commerce website which are competitors. Owner of first website take the prices of another website using scraping techniques and show his prices less than other which is illegal. In order to get rid of this problem, some defense mechanisms are designed. These defense mechanisms are of two types:-

1. Preventive Approach
2. Detective Approach

Preventive Approach

This kind of approach is used to prevent the bots from entering into the websites and stealing the important data. Various sites including Google, Amazon, Coursera etc. uses this approach for their data safety. Various techniques of preventive approach are:-

1. Manually
2. CAPTCHAs
3. Geo-Fencing
4. Flow Enforcement

Manually

During web scraping attacker HTTP request your server which further sends back the web page to the program. The attacker parses this HTML and extracts the required information. This process is repeated over and over again so that all the required information can be extracted from the website.

In order to get rid of this problem the webmaster can follow some steps:-

1. **Take a Legal Stand:** A person can clearly mention that web scraping is not allowed on this website. For instance Medium's terms of services contains following line:-

Crawling the Services is allowed if done in accordance with the provisions of our robots.txt file, but scraping the Services is prohibited.

The owner of website can take legal action against the potential attacker.

2. **Prevent Denial of Service(DoS) Attack:** After putting the legal notice there is a chance that attacker will again attack on your website. He/She can cause disrupt the daily services of your website causing DoS attack on your servers. To avoid this kind of situation you can detect the IP address of attacker and can block the requests coming from this IP address.
3. **Using .htaccess File:** .htaccess is the configuration file of Apache web server and it can help to prevent the scraping of your data. First you have to detect the attacker using Google Webmasters and then you can stop the attacker by doing some changes in configuration file.

CAPTCHAS

CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. This technique is used to detect whether the person entering the website is a bot or human with the help of images or text (Rahman et al., 2012). We can see when we enter any website it asks to write the text written in distorted form, this type of CAPTCHA was invented in 1997 by two parallel groups. CAPTCHA is efficient technique to prevent web scraping but sometimes it irritates the user also.

- You can design your own CAPTCHA by writing few lines of code but it is easier to use something like Google's reCAPTCHA in which user have to only tick a radio button and he can enter the website easily.
- If you are making your own CAPTCHA, try to hide its solution. If you provide the solution of CAPTCHA in its code it will become easier for attacker to decode it.
- Image CAPTCHAs can irritate the user easily as if there is some fault detected it will appear again and again.

Geo Fencing

Geo fencing is a technique in which websites are exposed only in some specific geographical regions where they do their business. This will not stop the web scraping but the attacker has to make extra effort because they have to run their web scraper over a specific geographic location. The attacker has to use the VPN link to a local Point of Presence (PoP-: Point at which two or more network build a connection between them) (Xing & Sieber, 2018).

Detective Approach

The Detective Approach is used to detect the bots entering into the websites to steal data and take defensive steps according to the behavior of these bots. Various techniques can be followed to stop the scraping of data (Rahman & Tomar, 2018).

1. Machine Learning Approach
2. Robots.txt Access Approach
3. User Agent Check
4. IP Address Approach

Machine Learning Approach

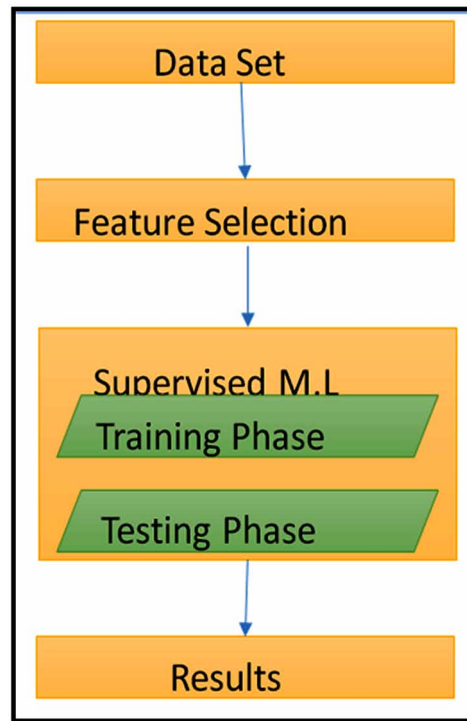
In machine learning approach we detect the behavior in which the bots are stealing our data. We take a dataset which includes the information about uses to differentiate between bots and humans. Database includes fields like time spent on a site, files scraped by any user etc. This database is passed to the supervised ML phase in which there are two phases like training set and testing set.

In training set the machine will be trained using above explained database and various training models like Naive Bayes, Decision Tree, SVM etc. and then testing will be done on other data. The machine learning process is shown in Figure 9.

Robot.txt Access

The Robot Exclusion Standard allows the Web Administrator to specify the part of site which is off-limits. Robot.txt includes the files specified by Web Administrator which are off-limits for robots which are going to attack the site. So, whenever robot visits any site, it should examine this file first. For instance, when a bot visit www.abc.com, the robot.txt file is accessed using the URL: <http://www.abc.com/robots.txt>.

Figure 9. Flow chart for the machine learning approach



Let us consider that the robot.txt file contains file named X.html which is not allowed to get accessed by the robot. But when bot comes to the site is scans each and every file related to the website. It will also go to X.html file and the bots get detected easily when they try to access robot.txt file. Any website does not provide direct hyperlink to this file from any HTML page, so many users are unaware of these files.

User Agent Check

When the bots do not work fine while scraping data it can cause the DoS(Denial of Service) and server will not be able to fine and there will be overloading on server. It is required to have a beneficial relationship between Web servers and bots. To establish a good relation between server and bot, the robot must declare its identity to the server. The User Agent field plays an important role which contains the identity of bot including its name. Sometimes bot designer uses user agent fields as that of Web browsers and detection of bot becomes very difficult.

IP Address Check

Another way to detect a bot is to match the IP address of Web client with web bots. This approach is not much useful as compared to other because the World Wide Web expands; it has become difficult to keep the record of all the bots coming onto the site. Also sometimes the web client uses the same IP address as that of the web bot. This approach is applicable only if the robot has been detected earlier. This doesn't mean that new robots could not get detected; new robots can be detected by examining the

top visited IP address and manually checking the origin of all the IP addresses. This approach is very time consuming and require more time and efforts than any other approach.

CONCLUSION

As described in the chapter, although there are great advantages of using web applications but there are lot of practical issues related to web application security needs to be answered. Similar to any technology, several security issues confront web applications. In this chapter security mechanism of Detective approaches and preventive approaches of web applications from web scrapping are reviewed, and the primary characteristics and elements of web scrappers are also explored. It is come out that scrapping attacks have a severe impact on web applications and the attacks may lead to the serious problem for web applications. Nearly all key attacks of scrapping in web application along with the feasible impacts and the existing countermeasures have been explained.

REFERENCES

- Abburu, S., & Babu, G. S. (2013). A frame work for web information extraction and analysis. *International Journal of Computers and Technology*, 7(2), 574–579. doi:10.24297/ijct.v7i2.3459
- Agrawal, S., & Agrawal, K. (2013). Deep Web Crawler: A Review. *International Journal of Innovative Research in Computer Science & Technology*, 1(1), 12–15.
- Cheng, F., & Evans, E. (2012). *U.S. Patent Application No. 13/447,986*. Washington, DC: US Patent Office.
- Cormode, G., & Krishnamurthy, B. (2008). Key differences between Web 1.0 and Web 2.0. *First Monday*, 13(6). doi:10.5210/fm.v13i6.2125
- Haddaway, N. R. (2015). The use of web-scraping software in searching for grey literature. *Grey J*, 11(3), 186–190.
- Herrouz, A., Khentout, C., & Djoudi, M. (2013). *Overview of web content mining tools*. arXiv preprint arXiv:1307.1024.
- Holmberg, R. J., Tlusty, M. F., Futoma, E., Kaufman, L., Morris, J. A., & Rhyne, A. L. (2015). The 800-pound grouper in the room: Asymptotic body size and invasiveness of marine aquarium fishes. *Marine Policy*, 53, 7–12. doi:10.1016/j.marpol.2014.10.024
- Johnson, F., & Gupta, S. K. (2012). Web content mining techniques: A survey. *International Journal of Computers and Applications*, 47(11).
- Mitchell, R. (2013). *Instant Web Scraping with Java*. Packt Publishing Ltd.
- Mitchell, R. (2018). *Web Scraping with Python: Collecting More Data from the Modern Web*. O'Reilly Media, Inc.
- Munzert, S., Rubba, C., Meißner, P., & Nyhuis, D. (2014). *Automated data collection with R: A practical guide to web scraping and text mining*. John Wiley & Sons. doi:10.1002/9781118834732

Myers, D., & McGuffee, J. W. (2015). Choosing scrapy. *Journal of Computing Sciences in Colleges*, 31(1), 83–89.

Ou-Yang, L. (2013). Newspaper: Article scraping & curation. Python Library. Retrieved.

Pak, C. (2017, May). News Company's Link Sharing on Twitter as Informative Advertising and Content Signaling. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 312-315). ACM. 10.1145/3027063.3027124

Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., & Markatos, E. P. (2010, October). Using social networks to harvest email addresses. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (pp. 11-20). ACM. 10.1145/1866919.1866922

Rahman, R., Tomar, D. S., & Das, S. (2012, May). Dynamic image based captcha. In *Communication Systems and Network Technologies (CSNT), 2012 International Conference on* (pp. 90-94). IEEE. 10.1109/CSNT.2012.29

Rahman, R. U., & Tomar, D. S. (2018). Botnet Threats to E-Commerce Web Applications and Their Detection. In *Improving E-Commerce Web Applications Through Business Intelligence Techniques* (pp. 48-81). IGI Global.

Rahman, R. U., & Tomar, D. S. (2018). Security Attacks on Wireless Networks and Their Detection Techniques. In *Emerging Wireless Communication and Network Technologies* (pp. 241–270). Singapore: Springer. doi:10.1007/978-981-13-0396-8_13

Usmanov, R. (2017). *Sběr, transformace a integrace dat z domény*. Academic Press.

Vargiu, E., & Urru, M. (2012). Exploiting web scraping in a collaborative filtering-based approach to web advertising. *Artificial Intelligence Review*, 2(1), 44.

Xing, J., & Sieber, R. E. (2018). Propagation of Uncertainty for Volunteered Geographic Information in Machine Learning (Short Paper). In *10th International Conference on Geographic Information Science (GIScience 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Yang, Y., Wilson, L. T., & Wang, J. (2010). Development of an automated climatic data scraping, filtering and display system. *Computers and Electronics in Agriculture*, 71(1), 77–87. doi:10.1016/j.compag.2009.12.006

ADDITIONAL READING

Ambite, J. L., Fierro, L., Gordon, J., Burns, G., Geigl, F., Lerman, K., & Van Horn, J. D. (2019). BD2K Training Coordinating Center's ERuDIte: the Educational Resource Discovery Index for Data Science. *IEEE Transactions on Emerging Topics in Computing*.

Assenmacher, D., Adam, L., Frischlich, L., Trautmann, H., & Grimme, C. (2019). Openbots. arXiv preprint arXiv:1902.06691.

Eiglsperger, M. (2019). New features in the Harmonised Index of Consumer Prices: analytical groups, scanner data and web-scraping. *Economic Bulletin Boxes*, 2.

Giulietti, M., Otero, J., & Waterson, M. (2019). *Rigidities and adjustments of daily prices to costs: Evidence from supermarket data (No. 1187)*. University of Warwick, Department of Economics.

Gunawan, R., Rahmatulloh, A., Darmawan, I., & Firdaus, F. (2019, March). Comparison of Web Scraping Techniques: Regular Expression, HTML DOM and Xpath. In *2018 International Conference on Industrial Enterprise and System Engineering (IcoIESE 2018)*. Atlantis Press. 10.2991/icoiese-18.2019.50

Kulkarni, A., & Shivananda, A. (2019). Extracting the Data. In *Natural Language Processing Recipes* (pp. 1-35). Apress, Berkeley, CA. doi:10.1007/978-1-4842-4267-4_1

Lewkowicz, J., & Celinska-Kopczynska, D. (2019). Web scraping and social media scraping—assessment criteria.

Riley, K. C. (2019). Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases. *Fordham Intellectual Property, Media and Entertainment Law Journal*, 29(1), 245.

KEY TERMS AND DEFINITIONS

Article Scraping: It is a process of scraping of the articles from the blogs or websites.

Content Scraping: It is a process of lifting off the displayed content from various websites and using it somewhere else or displaying it on other websites.

Data Scraping: It is a process used to extract massive amount of data from websites in which the data is stored in local computer system or in structured database.

Database Scraping: It is a process of directly extracting data from the database is known as the Database scraping.

Email Harvesting: The mechanism to obtain a large number of email addresses using different methods or techniques.

News Scraping: It is a process of scraping the news from the newspaper websites.

Price Scraping: It is a process of extracting or collecting the prices of various items in e-commerce site available over the internet without the consent.

Web Scraping: The process of extracting data from the websites in a systematic manner.

Social Engineering Using Social Networking Sites

Roberto Marmo

University of Pavia, Italy

INTRODUCTION

The protection of information is of vital importance to organisations and governments, therefore the development of measures to counter illegal access to information is an area that receives increasing attention. Information security is the specific discipline that regards the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

Even though the effectiveness of security measures to protect sensitive information is increasing, the human element remains a weak link because people remain susceptible to manipulation in order to obtain unauthorized information. Social engineering is the art of using human skills and persuasion techniques to obtain unauthorized information and to gain access to a myriad of sensitive services and data is called. Social networking sites are an ever more popular way for people to stay connected, in touch with other people across the globe, therefore a lot of social data are publicly available, a useful source of data to attackers.

The aim of this contribution is to describe some technologies and methodologies to execute social engineering using social media as specific approach, it also discusses background, knowledge, challenges and critical factors necessary for successful implementation or detection.

Background

A social network is a social structure made of individuals (organizations, company ecc.) also called nodes, which are connected by links represent relationships and interactions between individuals. Social networking sites are an ever more popular way for people to stay connected, in touch with other people across the globe. They become an integral part of personal lives. Business opportunities are formed and lost online. Social network is capable of holding all the private information that one feeds it with. It is thus the responsibility of a user to be accountable of the content one posts via the network.

Persuasion has always been part of human interaction. It can be used to influence and support good or improved behavior (Martin, 2014), but it can also be used to trick and manipulate people into performing actions that can end in some kind of loss, divulging confidential information (Mitnick, 2002) or giving money to fraudsters.

The brain creates routines, which can help deal with and process things more efficiently. But these routines can also compromise the ability to pay attention and to cause the brain to bypass details which would help detect fraudulent content. In addition to that, people generally believe that they are good at detecting social engineering attacks. Research, however, indicates that people perform poorly on detecting lies and deception (Qin, 2007; Marett, 2004).

DOI: 10.4018/978-1-5225-9715-5.ch054

Social Engineering

4

Social engineering is a process that cyber criminals use to psychologically manipulate an unsuspecting person into divulging sensitive details through the use of specific techniques. This approach is not enough to breach the security of an individual or a company, it is a fundamental step to obtain useful information to execute some successive malicious activity.

Social engineering is an extremely powerful tool that can be deployed to bypass complex and secure infrastructure and systems. It is superior to most other forms of hacking in that it can breach even the most secure systems, as the users themselves are the most vulnerable part of the system. Instead of technical attacks on systems, cyber criminals try to exploit the human's element of security and inherently psychological manipulation. In fact, according to a security industry survey, social engineering tops the list of the 10 most popular hacking methods.

Kevin Mitnick coined the term "Social Engineering" which has been repeatedly mentioned in several articles and papers on network and information security. There are various definitions of social engineering and also a number of different models of social engineering attack (Mouton, 2015, 2016).

The process of doing social engineering is known as a social engineering attack. Social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion.

Social engineering is deeply entrenched in both computer science and social psychology, knowledge on both disciplines is required to perform an attack.

A trivial example of a social engineering attack is when an attacker wishes to connect to an organisation's network (Mouton, 2016). As a result of his research, the attacker finds out that a help-desk staff member knows the password to the organisation's wireless network. In addition, the attacker gained personal information regarding the staff member who has been identified as the target. The attacker initiates a conversation with the target, using the acquired information to establish trust (in this case the attacker misrepresents himself as an old school acquaintance of the target). The attacker subsequently exploits the established trust by asking permission to use the company's wireless network facility to send an e-mail. The helpdesk attendant is willing to supply the required password to the attacker due to the misrepresentation, and the attacker is able to gain access to the organisation's network and achieve his objective.

The work of Mouton (2016) proposes detailed social engineering attack templates that are derived from real-world social engineering examples. The proposed social engineering attack templates attempt to alleviate the problem of limited documented literature on social engineering attacks by mapping the real-world examples to the social engineering attack framework. Mapping several similar real-world examples to the social engineering attack framework allows one to establish a detailed flow of the attack whilst abstracting subjects and objects.

The attacks of Kevin Mitnick (Mitnick, 2002) showed how devastating sophisticated social engineering attacks are for the information security of both companies and governmental organizations.

Social Network and Security

With the advent of social media and the Internet, social engineering has become easier and more commonplace. The creation of such attacks requires background information on targets. Individuals are increasingly releasing information about themselves online, particularly on social networks. The influx of employees using social media throughout the working environment has presented information security professionals with an extensive array of challenges facing people, process and technology.

The security behind social networks has become stronger in recent years, but relies mostly on the user to do the majority of the work in securing their identity and personal information from the outside world.

Numerous studies have shown that there is a growing correlation between social engineering and social media sites such as Facebook and Twitter, due to the wealth of personal and organisational information to be found within these environments (Furnell, 2008; Sanders, 2009).

More pointed attacks that target a specific person occur on social networks such as Facebook. These types of attacks make up over 39% of all social engineering attacks (Social engineering risks explored, 2011, September 22 from <http://www.continuitycentral.com/news05936.html>). These attacks look to find information on a specific individual to analyze and develop a social engineered attack against that person.

Cyber criminals, also called scammers, take advantage of human dependence on common social trust cues. They have been taking advantage of our human desire for news and social relevance to socially engineer us into giving away vital information.

A trivial example. If something has hundreds of Likes or Shares or if a friend had shared it, people mistakenly think it should be legitimate, people mistakenly think the information should be trustworthy. The scammers know this and they have used this to their advantage. Celebrity news is also always popular, especially fake deaths. While it may seem like an innocent hoax, it could have easily been exploited by cyber criminals to get you to click on a malicious link.

The work of Algarni (2017) aims to investigate the impact of source characteristics on users' susceptibility to social engineering victimization on Facebook. In doing so, we identify source credibility dimensions in terms of social engineering on Facebook, Facebook-based source characteristics that influence users to judge an attacker as per these dimensions, and mediation effects that these dimensions play between Facebook-based source characteristics and susceptibility to social engineering victimization.

Individual vs. Company Threats

Protecting the confidentiality, integrity and availability of information assets is a significant global business challenge for information security. Social engineering tries to manipulate your employees to gain access to valuable company assets. Information on employees of a given target company can be collected in an automated fashion and potentially misused for automated social engineering (Huber, 2010).

Businesses have a difficult job balancing company security and employee freedom on social media. While some business may have strict policies about what can/can't be shared on social networking sites like Facebook or Twitter, others don't have any policies at all.

Practices such as organisational engagement with social media and the publication of employee rosters on organisational websites are enabling attackers to easily identify an organisation's employees from amongst millions of social media users.

Approaches

Social engineering lifecycle try to obtain useful information to execute some successive malicious activity, it is composed of the following steps (Wilcox et al, 2014):

1. **Fact-Finding:** Social engineer tries to gather information that can then be used to build a relationship with the target important to the success of the attack;
2. **Entrustment:** Social engineer may exploit the willingness of a target to be trusting, in order to develop rapport with them;
3. **Manipulation:** The target may be manipulated by the trusted social engineer to reveal information or perform an action;
4. **Execution:** The target completed the task requested by the social engineer.

Phase-Base Model (Algarni, 2017) conceptualizes how the social engineer influences, persuades, and deceives victims. The success of attack is based on how well the social engineer performs the following eight phases:

- **Phase 1:** Using suitable gates of snss to gather information;
- **Phase 2:** Determining the tactic and developing a plan;
- **Phase 3:** Relying on one or more socio-psychological factors;
- **Phase 4:** Using suitable gates of SNSs to reach the victim;
- **Phase 5:** Wearing a suitable hat and playing a suitable character;
- **Phase 6:** Developing trust and a sense of safety;
- **Phase 7:** Choosing the perfect time;
- **Phase 8:** Using professional skills.

Source-Base Model (Algarni, 2017) is related to Phase 1 and Phase 4, in order to specify three sources or gates of threats:

1. Insecure privacy setting;
2. Friendship and connection with strangers;
3. Insecure dealing with content.

Different kind of techniques can be used, in order to obtain personal information using social networking sites, as described in following paragraphs.

App

Some social networking services like Facebook may allow you to add third-party applications based on API provided by social network platform (Srivastava, 2011), including games and quizzes, which provide additional functionality. Social media websites are advanced web applications, as their use requires a high level of interaction and capabilities.

A common form of attack is to entice users to authorize some third-party application, which is then given permission to access the user's personal information, post photos and status update, share link to your timeline or to any group you belong, post on behalf of you on the Facebook pages you own, access your, manage your page (Mayrhofer, 2013).

A study by the University of Virginia cites that out of the top 150 Facebook applications, all of which are externally hosted, 90.7% of applications needed nothing more than publicly available information from members. However, all of these applications were given full access to personal information not necessary for operation but supplied by the user granting the applications' total access to their account (Felt, 2009).

Moreover, Facebook warns that third-party apps could have been affected by recent breach.

It is necessary always beware of what permissions you give to a Facebook third-party application, even though Facebook is reviewing application's permission requests. Don't give permission to an application if you don't trust the website or application.

Data Re-Identification

Data re-identification typically deals with the linkage of datasets without explicit identifiers such as name and address to datasets with explicit identifiers through common attributes (Samarati, 1998). It has been shown that most of the US population can be identified through the combination of ZIP code, birth date and gender (Sweeney, 2000). Most Facebook users provide this information. Social engineers can take their data to estimate what their Social Security Number is.

Emails

One very common conduit for social engineering is scam and phishing emails. The email scam is an unsolicited email that claims the prospect of a bargain or something for nothing. The phishing email is message designed to look authentic and usually imitate format used by the trusted company, including their logo and branding. It will redirect the user to a fake site, that appears like the legitimate, but has a little different URL. In today's highly connected society an individual spends more time on the Internet or communicating by email. Due to large number of emails received, the brain creates routines, which can help deal with and process things more efficiently. But these routines can also compromise the ability to pay attention and to cause the brain to bypass details within the email which would help detect fraudulent content. So, scam and phishing emails can be highly disruptive.

Combination of three taxonomies is most commonly used in phishing (Ferreira, 2015): Cialdini's principles of influence, Gragg's psychological triggers, and Stajano's principles of scams. Principles of persuasion and people's negative emotions that are used in scam messages are defined in the work of Jakobsson (2016), it also describes automated countermeasures based on an understanding of the type of persuasive methods used by scammers.

Email from a friend can be used for attack, taking advantage of curiosity and trust. If a criminal manages to hack or socially engineer one person's email password, they have access to that person's contact list—and because most people use one password everywhere, they probably have access to that person's social networking contacts as well. Once the criminal has that email account under their control, they send emails to all the person's contacts or leave messages on all their friend's social network pages.

Many Facebook users have received phishing e-mails, and many have given the attackers private information such as login and password. An example of suspicious phishing e-mail:

Email subject: Your Facebook account has been blocked temporarily.

Dear Mister,

Your Facebook account has been blocked temporarily. It usually means that we need some more information about your account. Activate your account so we can confirm that you own the account

What do I have to do?

To activate your account, just click on this link and confirm your information. (It only takes a minute.)

Let's take a look at it in a bit more detail:

- email has not come from Facebook, because email address is different;
- spoof address used to make it look like someone else is using your account;
- some links lead to genuine Facebook pages;
- some links lead to a fake page to input your login details.

Without casting a sceptical eye over it, you might find yourself taking the information at face value.

Most email filters use techniques to identify email keywords, grammatical inconsistencies, typos or information misplacement. These can help email filters to have a wider range of detection but can also provide for many false positives since typos and inconsistencies are also frequent in legitimate human-written emails while with automatically generated emails, it may depend if the used template has mistakes or not.

However, the mentioned methods are effective only against the types of messages for which they were designed. Scammers are continuously changing the content of their emails to defeat these approaches, and their new content will not be recognized until the new signature is integrated within the filtering mechanisms. Scammers have increasingly come to realize that by cleverly targeting their victims, they can achieve even better returns. Thus, these prevention methods tend always to be one step behind the scammers.

To address this problem, it is necessary to widen the identification of scam emails through scrutinizing the persuasive content rather than just evaluating the form and structure. One approach to persuasion used by scammers involves the use of meaningful contextual information such as victims' online shopping or banking preferences, to make scam emails seem more appealing and trustworthy. Other persuasive elements such as logos, graphics, colors, or words and phrases that are recognizable by the recipients, can be employed to make dishonest emails appear legitimate and even personal.

False Friends

Social engineers can abuse the overall community trust by using the psychological deception of starting a friendship with the victim in order to build trust between the attacker and the victim. The main goal of any social engineer is to manipulate this trust to launch a premeditated attack. This is a simple and effective approach, because a third of social media users regularly accept unknown, unsolicited requests.

Most people when asked will agree that not everyone they know is their best friend; there are the mere acquaintances all the way to those with whom we share our deepest secrets, along with many shades in between.

Social networking sites has added new meaning to friends: two people are often friends or not friends. One may have a couple of close friends and thousands of distant friends, a social network may simply categorize them all as friends, but there are the mere acquaintances all the way to those with whom we share our deepest secrets, along with many shades in between.

There are two categories of malicious profiles or fake users. Minimally Invested Profiles are designed to target users who readily accept requests without doing any manual analysis of a profile, the social engineer will fill out the fields necessary to appear legitimate in a friend or connection request: name, picture, job title, and location;

Fully Invested Profiles are a more robust profile that is designed to fool just about anyone, the social engineer can spend considerable time filling out as much of the profile as possible, gathering connections to appear legitimate, and taking time refining and editing the profile to pass a basic screening.

More friends aren't necessarily a bad thing. The problem is who has access to our information? Social networking sites provide a certain level of access control, but most people do not take the effort to configure these properly. Therefore, everyone ends up with equal access rights to our information. It is necessary to consider that sometime information travels through several networks of friends, therefore it is possible that bad guys ends up with equal access rights.

Malware

Attacking a target with malware is easier than ever. Cyber attackers don't need to be computer programmers anymore, they can buy their malware on the dark web. A lot of the malware for sale is spyware like keyloggers and RATs (remote access Trojans).

Malware can then be hidden in file such as a photo, an audio file, or a document. The target won't see an executable filename, but an innocuous media filename, if the target views the photo, listens to the audio, or opens the document, the malware will execute on their PC or smartphone.

Malware on Facebook can take many different forms, but it most often manifests as a link being promoted or sent via Messenger to convince the user to click on a link that invisibly installs some malware. The main iterations of malware include the following:

- a friend ambiguously promoting a product or a service
- a message from a friend with a link or a video and a phrase such as "Is this you?" or similar
- any promotion, post, or message from a friend which seems dissonant with their tone or usual social media practices.

Automated Attack

Classic social engineering attacks are expensive, due to the fact that building and maintaining rapport with someone to finally exploit the relationship is a time-consuming task. The ultimate goal of automation is to reduce the human intervention time to a minimum.

Social Media can be evaluated as communication platform, by offering services such as private messaging and chats which can be used by automated social engineering bots. Automated social engineering bots require little human time resources, are scalable and thus make social engineering a cheap and promising attack (Huber, 2009).

The work of Huber (2009) introduces a high-level description of a possible software application for automated social engineering, using the attack segment of the cycle of deception as a framework based on automated social engineering (ASE) attack cycle.

OSINT TOOLS

The effectiveness of social engineering attacks can be greatly increased using Open Source INTelligence (OSINT) to boost the effectiveness of the deceptive ploys delivered in an attack (Jagatic et al., 2007).

A malicious user is perfectly capable of utilizing Facebook's advanced search function and cross reference user to gain access to hidden portions of a user's profile.

Simply Googling the company name with function such as `site:Facebook.com` or `site:Linkedin.com` or `site:Twitter.com`, employee names, products and commercial information can be found, and digging gradually deeper yields a mountain of information. In similar way, it is useful to search on Google the user social account.

Maltego is made by Paterva <https://www.paterva.com> and is a powerful tool to gather, combine and analyze OSINT on a target. Maltego provides a way to import or add data. It also provides transforms that can gather additional data using electronic methods.

Social Network Analysis

Social network analysis is a mathematical technique developed in modern sociology, in order to understand structure and behavior, to map relationships between individuals in social network, to study information flows.

The work of Vasconcelos (2013) deals with the possibility of social engineering attacks using footprinting performed through Social Network Analysis. Experiments were carried out using a Facebook user account. Various graph layout algorithms were studied and results with Fruchterman Reingold algorithm are demonstrated in this paper. An test user account was analyzed and graphs of the social network were produced allowing understand the group formation and behavior of actors in social networks, as well as information flow.

Proposed Solutions

The one mistake companies make that leaves them vulnerable to phishing attacks is not having the right tools in place and failing to train employees on their role in information security.

It is possible to harden yourself and your organization against social engineering attacks with education and by encouraging a healthy sense of skepticism, by spending some time reviewing a social network's privacy policy and understanding the default settings for your account.

The way to prevent attackers from acquiring false friend is to avoid people you don't personally know, even if they are friends of known friends, to require identity checks both online and in person to verify that a person is who they say they are, to avoid posting enough information on Facebook for false friends to be able to track you and know where you are and what you are doing all of the time.

Some huge red flags for recognizing a social engineering attack:

- Unsolicited call from someone claiming to be tech support;
- False urgency requests, don't fall for 'Act Now!';
- Fear can be a powerful motivator, don't fall for 'Help Me, I'm your friend and I'm going to be mad'.

Relevant ways to protect yourself are:

- Delete any request for financial information or passwords;
- Reject requests for help or offers of help;
- In email software set spam filters to high;
- Install anti-virus software, firewalls, email filters and keep these up to date;
- Set operating system to automatically update;
- Pays attention to the kinds of personal data they share on social media
- Frequent change of password, so hackers are not able to spoil account;
- Perform a regular backup to an external hard drive or the cloud, after backing up, disconnect drive to avoid malware to encrypt the backup drive as well;
- Social platforms give the user authority to control their privacy, by regulating privacy settings that display personal information.

Moreover, related to password, it is suggested to write your secret questions to wrong predictable answers. In this way, if a secret question what's your dog, you should not to write your dog real name, write only different answer like "thisissmysecretanswer". If you share your dog name, this protection saves your passwords.

In specific case of company threats, company culture based on security compliance and legal aspects is the best defense against social engineering scam, therefore it is recommended to:

- Establish social media policies and guidelines, regarding how social media participation will be applied to all of the members of an organization;
- Never post business information without permission, such as work schedule or photographs taken in the office;
- Increase employee awareness of the many tricks employed by social engineers against them in the workplace;
- Alerting employees to the high costs involved with brand and reputation damage;
- An endpoint protection system that can block the latest malware is, probably, best bet at stopping the attack.

Humans need to be trained, they are the weakest link. Companies should employ a training geared towards each kind of user, so that everyone is aware of the latest attacks. Employees should be tested by having an outside party conduct a social engineering test. These kinds of tests help keep the employee on their toes and more likely to avoid the attacks.

ETHICS IN SOCIAL ENGINEERING RESEARCH

Ethics is the study of morality. By providing principles and theories about different viewpoints about what is meant to be ‘right’, ethics helps classify arguments, defend a position or better understand the position others take and, in doing so, helps determine an appropriate course of action.

White hat hackers are knowledgeable individuals whose primary job is to understand a system from the inside out and this includes both the hardware and software sides of a system. These ethically certified hackers are instrumental in probing hardware and software systems for weaknesses. The tests that white hat hackers perform assess both computer system weaknesses as well as weaknesses in a business’ corporate IT policy.

Social engineering techniques are ordinarily performed on human participants, therefore it is necessary to think about the consequences of a variety of situations, ranging from agreeing the parameters of a test, to deciding which techniques should or should not be allowed during a test. In this way, the ethical impact on these participants needs to be considered, to ensure that harm does not befall those who participate in such research.

The work of Mouton (2015) identifies a number of concerns regarding social engineering in public communication, penetration testing and social engineering research. It also discusses the identified concerns with regard to three different normative ethics approaches (virtue ethics, utilitarianism and deontology) and provides their corresponding ethical perspectives as well as practical examples of where these formalised ethical concerns for social engineering research can be beneficial.

FUTURE RESEARCH DIRECTIONS

Defense strategies against automated social engineering attacks are a necessity and could form another cornerstone for future research. It is possible to study and design countermeasures which can be better equipped to target and minimize the success of specific types of attacks. The security measures of social networking sites are primarily concerned with unsolicited bulk messages. Emphasis must be given to new cyber education and awareness of users.

CONCLUSION

Social engineering has become a popular form of obtaining and utilizing confidential information in virtual communities and it is a fundamental step in various attacks to information systems. This chapter tried to bring some clarity to the different types of social engineering based on social networking sites.

Anyone in today’s modern world is vulnerable to social engineering and thus must remain constantly aware of who they interact with both online and in person, so it’s important to recognize an attack in progress and respond to it appropriately.

The problem is that, combined with social media, information harvested is easy to process and social engineering scams become increasingly more difficult to spot, because they’re coming from seemingly trusted sources: friends, professional references, and even family.

End users don’t understand that oversharing on social network channels can compromise more than their reputation.

To combat these new security threats, businesses need to apply new policies to protect their users and their information. To effectively guard against social engineering attacks, organisations must go beyond awareness initiatives and help end users actually make good security decisions and improve their cyber-hygiene using social networking sites, therefore cyber education is the key to success.

REFERENCES

- Algarni, A., & Xu, Y. (2013). Social engineering in social networking sites: Phase-Based and Source-Based models. *International Journal of e-Education, e-Business, e- Management Learning*, 3(6), 456–462.
- Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, 26(6), 661–687. doi:10.105741303-017-0057-y
- Felt, A., & Evans, D. (2009). Privacy protection for social networking APIs. *Proceedings of the Web 2.0 Security and Privacy W2SP 2009*.
- Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in social engineering and their use in phishing: Human aspects of information security, privacy, and trust. *Proceedings of the Third International Conference (HAS 2015)*.
- Furnell, S. (2008). End user security culture - a lesson that will never be learnt? *Computer Fraud & Security*, 4, 6–9.
- Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards automating social engineering using social networking sites. In *Proceedings of the 2009 International Conference on Computational Science and Engineering* (Vol. 3, pp. 117-124). 10.1109/CSE.2009.205
- Huber, M., Mulazzani, M., Schrittwieser, S., & Weippl, E. (2010). Cheap and automated socio-technical attacks based on social networking sites. *Proceedings of the 3rd Workshop on Artificial Intelligence and Security AISec2010*. 10.1145/1866423.1866435
- Jakobsson, M. (2016). *Understanding social engineering based scams*. Springer. doi:10.1007/978-1-4939-6457-4
- Marett, K., Biros, D., & Knode, M. (2004). Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training. *Lecture Notes in Computer Science*, 3073, 187–200. doi:10.1007/978-3-540-25952-7_14
- Martin, S. J., Goldstein, N., & Cialdini, R. (2014). *The small big: Small changes that spark big influence*. London, UK: Profile books Ltd.
- Mayrhofer, P. (2013). Interdependencies in the discovery and adoption of facebook applications: An empirical investigation. Springer.
- Mitnick, K. (2005). *The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers*. New York: Wiley.
- Mitnick, K., & Simon, W. (2002). *The art of deception: controlling the human element of security*. New York: Wiley.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186–209. doi:10.1016/j.cose.2016.03.004

Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, 55, 114–127. doi:10.1016/j.cose.2015.09.001

Qin, T., & Burgoon, J. (2007). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *Proceedings of the IEEE Conference on Intelligence and Security Informatics*, (pp. 152–158). 10.1109/ISI.2007.379548

Samarati, P., & Sweeney, L. (1998). *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and cell suppression*. Technical report, SRI International. Retrieved October 13, 2018, from https://epic.org/privacy/reidentification/Samarati_Sweeney_paper.pdf

Sanders, B. G., Dowland, P. S., & Furnell, S. (2009). An assessment of people's vulnerabilities in relation to personal and sensitive data. *Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance (HAISA 2009)*.

Srivastava, S., & Singh, A. (2011). *Facebook application development with Graph API cookbook*. Birmingham, UK: Packt Publishing.

Sweeney, L. (2000). *Uniqueness of simple demographics in the U.S. Population*. Carnegie Mellon University, Laboratory for Internal Data Privacy. Retrieved October 13, 2018, from <https://dataprivacylab.org/projects/identifiability/paper1.pdf>

Vasconcelos, L. E. G., Franco Rosa, F., Kusumoto, A. Y., Duarte, L. O., & Silva, P. A. L. (2013). Social network analysis for social engineering footprinting. In *Proceedings of the 8ª Conferência Ibérica de Sistemas e Tecnologias de Informação*, (vol. 2, pp. 185–190). Lisboa: Academic Press.

Wilcox, H., Bhattacharya, M. & R. Islam. (2014). Social Engineering through Social Media: A comprehensive investigation on enterprise security. *Applications and Techniques in Information Security, Communications in Computer and Information Science*, 243–255.

ADDITIONAL READING

Alomar, N., Alsaleh, M., & Alarifi, A. (2017). Social authentication applications, attacks, defense strategies and future research directions: A systematic review. *IEEE Communications Surveys and Tutorials*, 19(2), 1080–1111. doi:10.1109/COMST.2017.2651741

Monnappa, K. A. (2018). *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*. Birmingham, UK: Packt Publishing.

Ozkaya, E. (2018). *Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert*. Birmingham, UK: Packt Publishing.

Saxe, J., & Sanders, H. (2018). *Malware data science, attack detection and attribution*. San Francisco, CA: No Starch Press.

Talamantes, J. (2014). *The social engineer's playbook: A practical guide to pretexting*. Hexcode Publishing.

KEY TERMS AND DEFINITIONS

API: Application programmin interface, a set of subroutine definitions, communication protocols, and tools for building software.

Social: Engineer: A person who is expert on the social engineering techniques, he uses deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Social Engineering Attack: Various manipulation techniques to elicit sensitive information, manipulating a person into giving information to the social engineer.

Social Network: A social structure composed of individuals, organizations, company, etc. that are connected by relationships and interactions.

Social Network Security: The process of analyzing dynamic social network data in order to protect against security and business threats.

Social Networking Site: An online platform that allows users to create a public profile and interact with other users on the website.

Third-Party Applications: An application that is provided by a vendor other than the manufacturer.

User Account: An established technique for connecting a user and an information service.

Social Media and Identity Theft Implications on Nigerian Victims and International Economy

Tolulope Kayode-Adedeji

Covenant University, Nigeria

Obianuju Victoria Okeke

Covenant University, Nigeria

Lanre Amodu

Covenant University, Nigeria

Opeyemi Fasanya

Covenant University, Nigeria

Nelson Okorie

Covenant University, Nigeria

INTRODUCTION

In this 21st century and beyond, many can attest to the role of ICT in the development of communication in the world. According to Adaja and Ayodele (2013 p. 65), ‘one of the developments in Information and Communication Technology in the 21st century was the finding and advent of the new media which have enabled the formation of several channels of social communication.’

As a result of the fast-growing technology, in social communication, there has been dependence on the internet by a large percentage of individuals around the world.

Consequently, personal information is shared when creating profiles on social media platforms thereby making it easy for online crimes to take place. Security attacks such as hacking, identity theft, phishing scams, viruses are now common online as users share their names, date of birth, the name of schools, family information, and others on social media sites.

While activities online increase, there are concerns about the ways personal information shared by social media users may be collected and analysed (Hinduja and Patchin, 2009). According to Walker (2016) the state of the net poses, that more than half of the people using social media applications share private information about themselves online, exposing themselves to online dangers. The findings reveal that: 25% of persons with a *Facebook* account do not use the site’s privacy control or are not aware of them, 40% of social media users post their personal identity information online, exposing them to identity theft and 9% of social media users dealt with a form of abuse within the past year (e.g., malware, online scams, identity theft or harassment) (Finch, 2003).

Due to this increase, there seems to be a connection between the usages of such media with identity theft, cyberbullying, online sexual predators mainly affected youths because of lack of security consciousness and privacy about personal information (Jegade, et, al; (2016) McGillivray, 2015). Also,

DOI: 10.4018/978-1-5225-9715-5.ch055

committing identity fraud with the help of the Internet may be more accessible and more efficient for criminals than ever before (Milne et al, 2004).

Emily Finch, the author of “What a Tangled Web We Weave: Identity Theft and the Internet,” believes that social media users are “less security-minded about their personal information when they are online than they are in ‘real life’ situations.” This is true because when people are on social media sites, they reveal information online that they would not show to someone in real life situation. It is therefore easy to understand how this information is wrongly used and leads to identity theft (Finch, 2003).

Identity theft did not begin over the Internet. Before the use of internet became popular, fraudsters stole people’s identities by going through their documents. They also used their mobile devices to commit such fraud. In Nigeria, before the prominence of the internet, there were fraudsters commonly called 419’ers, and these fraudsters duped mostly big men and women who lived in Lagos (Ezea, 2017).

With the acceptance of internet, identity theft is becoming more popular around the world. According to Federal Trade Commission, identity theft was the number one fraud in 2008. Now with its popularity, different online fraudulent activities have become the norm over the years.

However, Nigeria social media users continue to fall, a victim of this fraudulent activities, as they continue to imbibe the culture of registration and to use newly established social media network with more existing features (Omodunbi et al., 2016)

Therefore, diverse investigation abounds on the issue of social media identity theft. Selwyn (2004) examined how older adult employed the uses of social media to lower perceived life stress thereby making them victims of social media identity theft. On the other hand, Rezmik (2013) investigates the dominant methods used in carrying out social media identity theft on social media networking site. They further stress the need for the Federal Governments to be solely responsible for the protection of social media users by ensuring the perpetrators are punished (Al-Daraish et al., 2014). Most importantly, Milne et al., (2004) discussed online behaviours that lead to identity theft to create awareness for online security for social media users.

To this end, Kayode-Adedeji et al., (2017) emphasized the need for regulating the social media, while Adu et al., (2014) further reviewed the different security and privacy risk threatening online social network users and proposed several systems that enable internet users’ activities to be monitored. Little research, however, has been done on the implication and users’ awareness of the necessary security measures social media users can put in place to avoid being a victim of social media identity theft.

Considering the differences that exist in countries, regarding the culture of communication on social media, the results emanating from this investigation gives a future opportunity for a comparative study serving as a guideline or map in the development of policies for future cybersecurity as emphasised by Peters (2017).

So, this research attempts to find out the implications of this crime on the victims, to ascertain if people are aware of this crime, to educate people on avoiding social media identity theft and also the reasons for such fraud.

ICT IN THE PRESENT AGE

Information and Communication Technology (ICT) inventions on the cyberspace remains over-whelming as more platforms are created to allow for diverse activities. There has also been applications (Apps), and websites, enhanced by new features on already existing internet environment. Communication technology has allowed the use of social media platforms, new features on gadgets, solar-powered drones,

apps, wireless routers LED (Li-Fi), and so on. Most of these above mentioned inventions and platforms increased the benefits the cyberspace already generates, making communication easier by providing people from different fields, with a more convenient approach of achieving task.

However, as the internet brings more advantages to user, some embrace these innovations for fraudulent activities and cybercrimes such as; cracking, software piracy, ponography, ATM fraud, *Yahoo-Yahoo* extortion, Identity theft, phishing which begins with fraudsters engineering applications and internet platforms for manipulation of users for unlawful gains. The Nigeria Cyber Security Report (2017) records that the desperate actions employed by fraudsters have resulted in the increase of cybercrime by 35 per cent between 2016 and 2017.

Nigeria presently lacks a working cybersecurity law. Maintain, O. Ogunleye, S. Ayinde, S. and Ad-ekunle, Y. (2013) from their research discovered that the rise in cybercrime in Nigeria has influenced drug trafficking, affected Nigerians image negatively, and encouraged plagiarism and infringement.

In light of the above stated information and implications, the book chapter seeks to address one of the major prevalent cybercrimes known as 'Identity theft', which involves the use of another person's identity to commit crime online. The chapter titled; 'Social media identity theft: The implications on victims in Nigeria' will be conducted with the sole aim of examining the implications of social media identity theft on victims and level of awareness on security measures on social networking platforms. In order to achieve these aims, the chapter engaged the knowledge of professional in the field of internet security such as programmers to provide original content on the recent methods employed by fraudsters in stealing others users' identity for fraudulent purposes. Victims of social media identity theft were interviewed from Nigeria to further understand their experiences, to educate other internet users for possible future attacks. Authors would be from relevant field namely: computer scientists, media communication, and criminology and security studies respectively.

The examination of the above areas of cybercrime, prepares internet users, ICT empowered organisations, and other Nigerian organisations who mainly engage the use of ICT, to defend themselves from internet attacks.

The results from the analysis could help reduce the negative effects on the dwindling Nigerian economy. The development of the internet and ICT will endure; therefore, it becomes imperative for computer programmers, social media platform providers and regulatory bodies that presently exist in few states in Nigeria to seek out ways to tackle problems that could be generated from online usage by online users. The results from the study is useful because it will encourage internet users to provide information online in cases of e-commerce because internet banking and transactions encourage international trade, therefore results from this study is useful. This will further drive necessary bodies, governments and organisation to begin to put in place necessary measure in curbing the act of identity theft and 'Catfishing' online.

History of Social Networking Sites

Things began to change rapidly in the 20th century as a result of the development of ICT. After the first supercomputers were created in the 1940's, scientists and engineers began to develop new ways to build networks of interconnectedness between the computers and these new ways led to the birth of the internet which we have today (Hendricks, 2013). CompuServe was the earliest form of Internet developed in the 1960's and also old forms of electronic mails were produced during this time. Communication via letters gradually became olden, as the networking technology during the 1970's improved with the invention of Usenet, which allowed users communicate through a virtual newsletter (Hendricks, 2013).

The first social media site was referred to as Six Degrees, and it was created in 1997. This social media site was conceptualized after the six degrees of separation theory, and it allowed users to create a profile and then become friends with other users who were registered on the site. It lasted from 1997 to 2001 (Hale, 2015). After the era of Six Degrees, the Internet transcended into blogging and instant messaging. Although, blogging was not a direct mode of social media communication, it allowed people to read articles and share opinions by commenting on such article. The term 'blog' was originated from weblog, and Jorn Barger coined it.

As the Internet became popular, more social media sites were developed. A social media site called Myspace became famous in 2003. Its main purpose was to connect people to become friends. Then, *LinkedIn* was developed, but it was geared towards a more professional setting that allowed different people from various walks of life to network and creates contacts for business purposes (Hale, 2015).

In 2004, Mark Zuckerberg developed *Facebook* as a Harvard student. According to a statistical report by Africa Internet statistics in June 2017, the number of *Facebook* subscribers in Africa was 1,979,703,530 billion. Then in 2006, *Twitter* was created by Jack Dorsey, Biz Stone, Noah Glass and Evan Williams. It allows users to send tweets and also send messages to their various followers. After the creation of *Facebook*, *Twitter* and some other social media sites became prominent with the same functions while few social media sites had little features that made them distinct. Social media sites like *Flickr*, *Photobucket*, *Instagram*, and *Snapchat* provide features that distinctively allow users to share pictures, and also allows users to chat with their friends around the world.

Tumblr was introduced in 2007 by David Karp, and it was a microblogging site, and also it allowed users to communicate with one another while sharing articles, pictures, videos that were of interest to the users. *Yahoo* was developed in the late 2000's, and it later bought *Tumblr*. Other social media sites that have taken over the social space over the years are *Blippy*, *Loopt*, *Groupon*, *Buzz*, *Google*, and many others. As a result of the fast-growing fame of social media platforms, people started using these sites as a form of advertising businesses. So, social media platforms were not only for users to communicate with one another but also business owners used social media platforms as a marketing and advertising platforms.

Today, there are thousands of social media platforms that have taken over the social space, and these platforms help in communication and have specific features that make them distinct from one another.

The Nature of Social Networking Sites

Social networking sites are internet or mobile-based social space that allows people to connect, communicate, create and share content with others. People engage social media to interact with friends, family, organizations, and the world. It enables people to send instant messages, find friends, join online groups, and share photos, videos, opinions, articles, web information, stories, and more.' These actions explain the automatic freedom social media gives to users to create their profile pages and share contents.

Stutzman (2007) opines that there are various types of social networking sites. They are divided into two. Some sites-based solely on the users' profile and information and the other focus exclusively on users building their content.

The profile based social networking sites are built and organized around users' profile pages. *Facebook*, *Myspace* are perfect examples of this type of sites. Users enhance their pages in different ways and also contribute to another users' page.

In the content-based sites, a user's profile page is an essential means of organizing relationships and networks but also is vital to the way a user posts content on social networking sites. *Instagram*, *YouTube*, and *Snapchat* are good examples here because relationships are based on the people who comment on videos or pictures a user upload.

The social media space is developing rapidly, as people around the world are being acquainted with the way social media operates and functions. Social media networks give users the room to manage and build networks of friends via the Internet, and these friends can be individuals, businesses, events and other things. However, it primarily enables one to build an online network base and keep in daily contact with these created networks. Social media networks allow users to freely add anyone as a friend, or some friends have to be made on request in which the two parties have to acknowledge the fact that they know each other.

Permission is an important feature of most Social networking sites. It allows members and groups to control who gets access to their profiles, information, connections and spaces. This setting allows users to keep information private, or to make information public. Through these combinations of permissions and privacy, users can manage a range of different relationships online, as well as managing their online presence.

Another important feature that all social media network sites have is the friend request or follower request feature. Security measures on social media networks differ from status to status, although basic security measures are enabled by social media platforms. There are settings that allows users to keep personal information private and it is only visible to friends on the user's contact list and can even restrict information to some particular friends. Through security settings, users are able to control the way they handle relationships online via social media networks, and their online presence.

Social networking sites also differ based on the functions they provide to the users. Generally, they are used for communicating but each media still has its distinct function(s). According to Boyd and Ellison (2006), Social networking sites have three common elements: a member profile, the ability to add friends or people to a contact list and supported interaction between members of the contact list.

Impact of Social Networking Sites on Users

The different Social networking sites have made impacts on communication, social cohesion, community engagement, business, social relations, crisis management and a whole lot more. These impacts vary from good to bad. Social networking has become a part of the daily life experience for an increasingly number of people. (Gemmil, and Peterson, 2006). Social media is the environment in which social networking takes place and has altered the way consumers gather information and make buying decisions.

Beebe, Beebe, and Redmond (2005) reveals that conversation between family members have being altered by technology. Social networking sites being a part of the internet has altered the world of communication by helping users communicate timely, accurately in clear messages. The Social networking sites has evolved from sharing information, pictures or videos to interacting, engaging and networking. The fact that the social networking sites has altered the means of communication does not leave the terrestrial medium of communication useless. Rather it has allowed real time broadcast and has aided citizen journalism by enhancing free flow of information, eyewitness account and freedom of information. The change in communication by social networking sites have revealed the applicability of social networks in everyday life.

Almost 4.2 billion individuals connect to social networking sites via their mobile devices and this shows that the social networking sites are relevant to people differently. The sites have made it possible to develop social relations with people of similar interests and connect people across the globe without any geographic, economics or political barriers. As identified by Kaplan and Haenlein (2010), the basic keys to social media success are user participation and user interaction. Weinberg and Pehlivan, (2011) also reveals that people with different backgrounds can engage in long-term discussion because social networking sites reflect views, richer conversation and long-term engagement. With this said, Social Networking Site (SNS) is a process of becoming more acquainted with people, encourages long-term relationship and help to strengthen communication among families, business partners and even friends. However, as much as SNS have positively influenced social cohesion, it may also bring an unpleasant experience on online behavior as people have the tendency to behave differently based on the person they are sharing information with. In the process of social relations with people (strangers) Social media users are susceptible to social vices such as cybercrimes, cyber bullying, pornography and some are even impersonated as they tend to share information about themselves to strangers they meet online. Adolescents especially are easily influenced by what they see on SNS most especially the perception of how other people live their lives making them feel inferior and also start believing that other people have better lives than they do.

Furthermore, as people most especially teenagers join SNS to keep up with their social Life, adults and organization especially use the platforms to promote their business and brands since SNS gives opportunity for cheap advertisement. Social networking has positively and negatively impact buying and selling has most business is known through the social media platforms. SNS like Facebook and Instagram have a different platform for businesses where organizations can upload contents about their businesses and sponsor those contents to a particular number of people who are likely to patronize their services. Business with SNS are likely to attain successful results compared to business without social media platforms. So, while the customers (social media users) move with the trend, organizations also make the shift as their customers are easily available on the platform. As much as SNS is used to promote businesses, it has also helped organizations to manage crisis and misunderstanding. Freberg (2012) in his study stated that the viral spread of information on social media could be viewed as an advantage to a crisis professional who must reach the public as quickly as possible. However, social networking sites can only have great impact on business if the right audience is targeted and reached.

As much as SNS has encouraged E-commerce, E-banking and E-governance, it has also negatively affected some business. Some business profiles have been hacked, some are impersonated by fraudsters who make followers believe it is the original platform and then making them pay for a product without getting the delivery.

Social networking sites has revolutionized our ability to connect and collaborate in ways we could not have fathomed five years ago. Students, businessmen and all other professionals can collaborate through web 2.0 as well as social networking sites. Students' collaboration could be used to aid the process of working with others. Students can post ideas through instant messaging like *WhatsApp*, *Gmail* and get feedback from whom they are working with. They can also brainstorm to narrow or expand concepts. They can discuss ideas, share ideas and collaborate on a project. An example is research clusters. They can always have their meeting on the SNS platform. Programmes and discussion are also done through the social media platforms like *WhatsApp* where you have discussion programme with a fixed time.

Through Social Media, virtual proximity has become a substitute of physical proximity in the case of standard transactions. Generally speaking, network externalities appear when the last person connected to the network, due to his/her participation, ensures the increase in utility for all the users. Content creators, such as teachers, can place special interest in creating positive interactions between their target audience and social networks to improve their attitude towards media. Such highly involved interactions between users ideally create positive experiences toward learning.

Social Media Identity Theft in Nigeria

Identity theft occurs when an individual, a perpetrator uses another person's information for illegal purposes. Identity theft takes various forms like financial, criminal and medical identity theft. Financial identity theft includes activities that tamper with one's credit card information. Criminal identity theft is used to commit crimes in another person's name and to carry out financial crimes in another person's name. (Michael et al., 2014). Social media identity theft is a form of cybercrime in Nigeria, although most research have not documented the level of its existence.

Fraudsters obtain people's information through an act called dumpster diving. Important documents may include bank statements, receipts, NEPA bills, ATM card papers, and many more. When these documents are retrieved, vital information such as: date of birth, full name, mother's maiden name, ATM pins, passwords, driver license numbers amongst others.

In Nigeria, Social networking sites have reached a high mark such that every sector including banks, organizations, business owners, schools, government, use these sites to promote business and communicate with the public. Social networking sites like *Facebook*, *Twitter*, *Snapchat*, *Instagram* and others serve as a platform through which fraudsters engage in such fraudulent activities. There are many reasons associated with people would becoming fraudsters on Social networking sites, and they include: unemployment, yearn for more money, the absence of efficient cyber laws in the country, and Lack of security measures put in place by individuals on computers and many more.

Identity theft in Nigeria ordinarily started with '419,' which was a popular form used by fraudsters to collect money from unassuming victims. This is carried out in a way that the fraudsters would pretend to be people who they are not and thereby swindle the victims unknowingly. Today, social media identity theft occurs on social media platforms like *Twitter*, *Facebook*, *Instagram*, *WhatsApp*, *Snapchat*, *LinkedIn*, *IMO*, and others (Michael et al., 2014).

With the advancement of technology, especially in the area concerning the internet, new ways to steal people's identity keep springing up and it is becoming harder by the day to actually stay secure and protect personal information. The use of social media platforms in Nigeria is still a growing phase and therefore a lot of persons are apathetic about the risks that come with sharing some sorts of information including pictures and videos online (Rezmik, 2013). It is important for people to be aware of security checks and measures to take note of when creating user accounts on Social networking sites. Some of these measures include:

Creating strong passwords: when creating an account on a social media-networking site, it is important to ensure such passwords do not contain information about you. They should contain capital letters, small letters, symbols, and numbers. Passwords should be changed from time to time and kept away from the public.

Table 1. Implications of social media identity theft

RESPONSE CATEGORIES	PERCENTAGE (%)
Loss of Social Media Account	47.1
Financial Implications	18.1
Loss of Friends Contact Online	21.0
None That I Know Of	13.3 n= 210

Secondly, give minimum information when filling out forms online to create accounts on Social networking sites, not all fields are necessary to fill. Social media users are also encouraged to be careful about what pictures, videos, and information they post on their status and use privacy settings. There should be a regular check on google to trace any forged accounts that may be operating with one's details and avoid accepting friend requests from strangers.

METHOD

The qualitative and quantitative research design was adopted. Interview and questionnaire were used as a method to gather data for the study. A total of 210 victims of identity theft completed a copy each of the questionnaire. Also, for the qualitative data, a focus group discussion consisting of 3 male and 3 female victims of social media identity theft were interviewed. A programmer was also interviewed to further examine diverse methods used by perpetrators to carry out social media identity theft.

The Uses and Gratification Theory

This theory was propounded by Elihu Katz in 1970 which states that the audience use the mass media to satisfy their certain needs (Onwubere, 2004). This means that the audience are not participatory individuals of the media, so they select the media messages that satisfy their needs, wants and gratify them.

According to Severin and Tankard (1987), different people can use the same mass communication message for different purposes. The Uses and Gratification theory is relevant in this research because this theory explains how persons use social networking sites to gratify their communication needs and wants. In the case of this study, fraudsters use other people's identity especially on social media sites to satisfy their needs ranging from financial benefits, stalking and to embarrass others.

Social networking sites provide its users a wide option of communication channels either through texting, video calls, audio calls and many more and it beats the issue of geographical barrier, so its users are always online to connect with people from around the world or for other purposes. This makes the availability of improved information to users all the time. This theory is relevant to examine how users make use of social networking sites to gratify their needs but also doing so at their own security cost.

Results

The table above shows that 47.1% are of the opinion that the implications of social media identity theft leads to loss of social media account, 18.1% are of the opinion that the implication leads to financial implications, 21.0% are of the opinion that the implications of social media identity theft leads to loss of friends contact online, while 13.3% are not sure of the implications of social media identity theft on them.

According to the table above, the implications of social media, identity theft mostly leads to loss of social media accounts. The other implications of social media identity theft are financial implications, loss of friends contact online. These implications could mean that the original owner of the account may not be interested in using the account again if necessary actions are not taken, by the social media platform providers. From the focus group interview conducted, it was observed that most of the participants were either embarrassed or sad when they realized that they had fallen victim of social media identity theft. Most people who are victims of social media identity theft, do not realize initially that they have fallen victim at times until their attention is drawn to whatever activity their page is being used for.

According to respondent A:

Okay, I saw a post that was not mine.... It was a nude picture of Kim Kardashian that was posted... My family started asking me if I had gone on the dark side because of the nude pictures, and they started asking me what I was doing, what I was uploading and my religion was questioned at that time.

Also, according to respondent B:

I was devastated and angry. Yes, I lost the account and I was angry. I lost a lot of friends and I kept thinking of how to upload pictures and also how to retrieve the ones I had uploaded in the past. I also had to open another account and that was stressful.

According to respondent C:

My friend told me about it and I reported after which, the account was blocked, but I had to create a new account and it was stressful. I had to start sending friend requests all over again but now I am back where I was as at the time my identity was stolen.

Also, according to respondent D,

The implication was devastating. As with my snapchat, I could not recover the account, I lost my friends and contacts online, but I have gotten over it.

Different Ways in Which Social Media Identity Theft is Carried Out?

The result shows that there are various methods like phishing, forgery, social engineering, phishing sites, pop-ups, and others. Phishing according to one of the respondent A:

Table 2. Respondents awareness of security measures on social networking sites

Response	Percentage (%)
Yes	65.7
No	27.1
Not Sure	7.2 n= 210

... and here, people send mails to people and it is really going on in Nigeria now whereby you see messages in your emails, text messages on your phone, telling you that they want to get information about your bank details. So, phishing is just emails and messages sent to you pretending to be an official company or an official site trying to get vital information from you and some people fall victims of such tricks.

In this case, the possible victim sees messages in their emails, messages on their phones requesting for some information or personal information, such as bank details.

So, pop-ups do not really have to request for information from the target, rather it comes in form of dialogue boxes and once it is clicked on it downloads information from the device and such information becomes used by the perpetrator. According to respondent B,

Perpetrators can just create pop-ups...Some are not adverts, some are actually meant to infect your system when you click on it like when you click on the site, you see something different from the original site, and during that time something has downloaded into your system, and at times you see the thing downloading but when you open the download and see nothing you think it is actually nothing and you leave it that way, but something is in the system and it is till when you use anti-virus that it removes.

Social engineering as a method operates on online forums, blogs, online communities and so much more. It is done on any platform that generates a lot of comments from its users. According to respondent B,

Social engineering is making use of social platforms, basically things that people communicate with, anything that is social and anything that plenty people make use of to communicate with each other and to pass information online like forums too.

Phishing sites are fake sites that look like the original site and a user is not aware of the difference and then puts all of his or her information without knowing that it is the fake site of the original site and through this way perpetrators or fraudsters can illegally gain access to a person's personal information. Phishing sites according to respondent A, is

...these sites pretend to be clone sites of an original site...So, the cloning site would ask for a lot of details and they store these details. The one that is common in Nigeria is the banking way, the fraudsters send sms to your phones informing one that his or her BVN number is wrong so send your details, or that his or her ATM card has issues and sometimes it is also done through emails too. So, you visit this site thinking you are on the real site whereas it is a clone.

Table 3. Respondents' Security Measures on Social Media Identity Theft

RESPONSE	PERCENTAGE (%)
Privacy Settings	73.8
Rejecting Requests from Strangers	7.1
Minimize Basic Information About Yourself	5.2 n= 210

A high number (65.7%) of respondents are aware of security measures on social networking sites, 27.1% respondents are not aware of security measures on social networking sites, while 7.2% are not sure if security measures exist on social networking sites.

According to the table above, most respondents are aware of security measures on social networking sites, and according to the table below, most respondents are more aware of privacy settings as a security measure.

A total of 73.8% of the respondents are more aware of privacy settings as a security measure, 7.1% respondents are of the opinion that not accepting requests from strangers is a security measure, while 5.2% are of the opinion that not putting any basic information about yourself is also a security measure.

Some other security measures include, not accepting requests from strangers, not putting any basic information about yourself, not posting pictures, videos or chatting with friends.

From the interview session, according to respondent A,

But once you accept someone as your friend, they can view anything you post. So, privacy settings are not a form of security against people who are trying to steal your identity they are just privacy settings so, most of these sites what they think of first is their money before any other thing.

Most people are aware of these privacy settings but not a lot of people actually use these settings on their social networking pages. Most people are mostly used to changing passwords if they do not close down the account or lose the account. According to respondent A in the interview session:

So, we tell people to use strong passwords, do not use the same email on your social media page because if you have your email with your social media they can hack your page and also hack your email too using the same password.

According to respondent B, from the focus group interview;

I have not done anything so serious apart from changing passwords.

Also, according to respondent A,

Well me I also do the same thing of changing my passwords, but I change my passwords every week.

CONCLUSION AND RECOMMENDATIONS

This research is titled “Social media identity theft: The implications on victims in Nigeria” and the topic was inspired by the increasing rate of identity theft on social media, i.e. Social networking sites. Most people refer to it as hacking, and they mean more or less the same thing but social media identity theft is more technical and it encapsulates the exact activity that is associated with it. The main purpose of this study is to examine the various implications victims face, implications and security measure adopted as a result of this fraudulent activity. It can be gathered from the research that social media promotes identity theft and its implications on victims are more negative than positive. From the different methods used for this study, one primary thing observed is that the stringent security measures expected to be present on these social networking sites are not as useful as they are supposed to. There are security measures like privacy settings but according to an expert this type of security measure is not effective and it still leaves users prone to online danger like social media identity theft.

One of the experts who was interviewed is of the opinion that most social media sites do not care about the security of their users but rather they are more concerned with how much profit they make from the users in any way. According to the respondent A,

“...most of these sites what they think of first is their money before anything other thing. There is something I read about a guy whose Facebook account was cloned, whereas he had previously shut down the Facebook account and he found out later that the same page he shut down was somehow active still bearing his pictures, information and all, so someone already stole his identity. What actually happened is that when you request for your Facebook account to be shut down, it goes through a process for like a week so it does not shut down immediately. During that week process if you try to send a message or activate the page again, it is going to stop the process of shutting it down so the page will still remain active. And this happened in U.S and the victim said he contacted Facebook and even sent them emails and they told him that their support service will get to it and all, and nothing happened till he contacted the FBI, and told them everything about it and then few hours later the page was shut down.”

Apparently, social media identity theft is common on *Instagram*, a social media networking commonly used. Therefore, avid social media users should be able to determine and control the information to share and with whom such information is shared with. Users of social networking sites should also learn to use strong passwords on their accounts and be careful whom and which sites they share their passwords with to avoid being victims of social media identity theft. It is important for the government to provide security measures in order to protect the citizens against such fraudulent activity in the future by punishing perpetrators. Lastly, social networking site providers should be actively involved by making sure their social platforms are updated to ensure future safety, provide a platform to educate citizens on the importance of online security and how to stay safe in today’s world.

REFERENCES

- Adaja, T., & Ayodele, A. (2013). Nigerian youths and social media: Harnessing the potentials for academic excellence. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 2(5), 65–75. doi:10.12816/0001189
- Al-Daraiseh, A. Al-Joudi, A., Al-Gahtani, H., & Al-Qahtani, M. (2014). Social Network's Benefits, privacy, and Identity Theft: KSA case study. *International Journal of Advanced Computer science Application*, 5(12), 129-143.
- Beebe, S., Beebe, S., & Redmond, M. (2005). *Interpersonal communication: Relating to others* (5th ed.). Boston: Pearson.
- Boyd, M., & Ellison, B. (2007). Social Network Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 201–230. doi:10.1111/j.1083-6101.2007.00393.x
- Ezea, F. (2017). *An overview of Internet Governance and Infrastructure in the Philippines*. Foundation for Media Alternatives.
- Finch, E. (2003). What a tangled web we weave: Identity theft and the Internet. In Y. Jewkes (Ed.), *Dot. cons: Crime, deviance, and identity on the Internet* (pp. 86–104). Collompton, UK: Willan.
- Freberg, K. (2012). Intention to Comply with Crisis Messages Communicated Via Social Media. *Public Relations Review*, 38(3), 416–421. doi:10.1016/j.pubrev.2012.01.008
- Gemmill, E., & Peterson, M. (2006). Technology use among college students: Implications for student affairs professionals. *NASPA Journal*, 43(2), 280–300. doi:10.2202/0027-6014.1640
- Hale, S. (2014). Global Connectivity and Multilinguals in the Twitter Network. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY: ACM. 10.1145/2556288.2557203
- Hendricks, D. (2013). Complete History of Social Media: Then and Now. *Small Business Trends*. Retrieved from <http://smallbiztrends.com/2013/05/thecomplete-history-of-social-media-infographic.html>
- Hindiya, S., & Patchin, W. (2009). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206–221. doi:10.1080/13811118.2010.494133 PMID:20658375
- Hinduja, S., & Patchin, W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence*, Vol, 31(1), 125–146. doi:10.1016/j.adolescence.2007.05.004 PMID:17604833
- Jegade, A. E., Adejuwon, G. A., Olowookere, E. I., & Elegbeleye, A. O. (2016). Ecological Approach to Nigerian Youths Cyber-Fraud Participation. *Social Sciences*, 11(22), 5284-5293.
- Kaplan, M., & Haenlein, I. (2009). *Users of the world, unite! The media challenges opportunities of social media*. Kelly school of Business, Indiana University.
- Kayode-Adedeji, T., Oyero, O., & Aririguzoh, S. (2017). *Regulating the social media for global relationships*. Paper presented at the 4th International Conference on Education, Social Sciences and Humanities, Dubai, UAE.
- McGillivray. (2015). *What are the effects of social media on youths?* Retrieved from <https://turbofuture.com/internet/effects-of-social-media-on-our-youth>

Michael, A., Boniface, A., & Olumide, A. (2014), 'Mitigating Cybercrime and Online Social Networks Threats in Nigeria: *Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz*, 22–24.

Milne, G., Rohm, A., & Bahl, S. (2004). 'Consumers' protection of online privacy and identity'. *The Journal of Consumer Affairs*, 38(2), 217–232. doi:10.1111/j.1745-6606.2004.tb00865.x

Omodunbi, A., Odiase, O., Olaniyan, M., & Esan, O. (2016). Cybercrimes in Nigeria: Analysis, Detection, and Prevention. *Journal of Engineering Technology*, 1(1), 37–42.

Peter, A. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*.

Rezmik, M. (2013). Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. *Touro Law Review*, 29(2), 455–483.

Selwyn, N. (2004). The information aged: A qualitative study of older adults' use of information and communications technology. *Journal of Aging Studies*, 18(4), 369–384. doi:10.1016/j.jaging.2004.06.008

Severin, J., & Tankard, J. (1987). *Communication theories: Origins, Methods, Uses*. New York: Hastings House.

Stutzman, F. (2006). An evaluation of identity-sharing behaviour in social network communities. *Journal of the International Digital Media and Arts Association*, 3(1), 10–18.

The Citizen Lab. (n.d.). Retrieved from <https://www.fma.ph/2017/04/25/new-report-overview-internet-infrastructure-governance-philippines/>

Walker, K. (2016). Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection. *Journal of Public Policy & Marketing*, 35(1), 144–158. doi:10.1509/jppm.15.020

Weinberg, D. B., & Pehlivan, E. (2015). Social spending: Managing the Social Media Mix. *Business Horizons: Kelly School of Business*, 54(3), 275–282. doi:10.1016/j.bushor.2011.01.008

Online Phishing and Solutions

4

Ping Wang

 <https://orcid.org/0000-0003-0193-2873>

Robert Morris University, USA

Anteneh T. Girma

University of District of Columbia, USA

INTRODUCTION

Online phishing is a common form of criminal attempt via fraudulent emails, web links and websites to trick online users to surrender sensitive private information, including user names, passwords, social security numbers, credit card numbers, and bank account numbers. Phishing continues to be a primary weapon used by cybercriminals. Phishing is often used as the lead action followed by malware installation or other malicious actions that lead to a data breach. Statistically, 85% of organizations have reported being the victim of a phishing attack (Wombat Security, 2016). Spear phishing email, one example of phishing, was the starting point that led to 91% of successful cyberattacks and the resulting data breach (PhishMe, 2016). In addition, phishing was involved in 70% of all data breaches associated with nation-state or state-affiliated actors (Verizon, 2018).

Phishing attempts may occur in various formats, including email scams, malicious attachments, and fraudulent links and websites. Phishing in nature is a form of social engineering attack that exploits human vulnerabilities of curiosity and lack of awareness and judgment. Individual curiosity and lack of awareness often lead online users to become victims of spoofed and deceptive emails, fraudulent web links and fake websites (Alexander, 2016; Gupta, Arachchilage, & Psannis, 2018). Research on predicting individual susceptibility to phishing shows that certain behavioral traits are correlated to the ability to identify phishing interfaces; it also shows that individuals with greater behavioral curiosity tend to commit more security errors in identifying phishing attempts (Chen, YeckehZaare, & Zhang, 2018).

Online phishing has various types of significant impact on organizational and individual victims. The average direct financial cost of a phishing attack to an organization is over \$3.7 million, which is close to the cost of a typical data breach (Ponemon Institute, 2017; Wombat Security, 2015). The costs may include direct loss of productivity and revenue, business disruptions, and costs to contain malware and credential compromises. Additionally, there may be substantial hidden and indirect costs such as damage to corporate reputation and loss of customer confidence as a result of the data breach caused by a phishing scam (Anderson et al., 2012). Phishing scams are a leading cause for individuals to fall victims of identity theft. Over 17 million individuals in the United States alone were victims of one or more incidents of identity theft in 2014, and the majority (86%) of them experienced fraudulent use of their existing credit or bank account information (US Department of Justice, 2017).

DOI: 10.4018/978-1-5225-9715-5.ch056

To combat online phishing, a variety of countermeasures have been proposed, including education and training, improvement of administrative and security policies and practices, as well as technical solutions and software products. This chapter proposes a comprehensive solution to prevent and protect against online phishing. The following sections will define and describe various categories and types of online phishing, explain the theoretical principles for phishing and how each type of phishing works, and propose and discuss a comprehensive set of solutions, mechanisms and best practices to defend users and organizations against online phishing.

BACKGROUND

The term “phishing,” with a “ph” from earlier phone phreaking to replace the “f” in “fishing,” was first used in 1996 by hackers who were stealing passwords for America Online (AOL) accounts from unsuspecting AOL users, and the first media publications warned consumers about the “phishing” threat in 1997 (Gupta, Arachchilage, & Psannis, 2018; Ollmann, 2017). The earlier concept of phishing was limited to the use of email scams by online criminals to “phish” for passwords and financial data from a sea of Internet users (Ollmann, 2017). But the definition of the phishing has been evolving with various versions. Based on a systematic review of 113 definitions of phishing, Lastdrager (2014) tried to propose a consensual definition: “Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target” (p.8). This definition identified and emphasized the important core concepts of deception, impersonation, information, as well as scalability for mass distribution.

The Anti-Phishing Working Group (APWG), a non-profit international research foundation that specializes in the study of phishing and cybercrime, provides the following definition of phishing that offers a more specific and enlightening focus and directions on the nature and techniques of phishing: “Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials” (p.2). The social engineering component of phishing highlights the nature of victimization by exploiting human weaknesses in phishing. The specific technical subterfuge, or mechanisms and methods of deception, may include using spoofed emails, planted crimeware or malware, online interception systems, or phisher-controlled keyboard interception to trick consumers and steal their sensitive information (APWG, 2018).

Social engineering in the context of online crime is defined as “an umbrella term for a broad spectrum of computer exploitations that employ a variety of attack vectors and strategies to psychologically manipulate a user” (Heartfield & Loukas, 2015, p.1). Social engineering primarily targets human users and exploits human psychological weaknesses. The computer exploitations and attack vectors and strategies include examples of technical subterfuge in online phishing to trick and deceive human users. In *The Art of Deception*, Kevin Mitnick, a former master phisher, concluded that the human factor is the weakest link in security and that successful social engineers usually have strong people skills to win and exploit trust from potential victims while most people believe in and behave with trust and love for each other with a low level of suspicion (Mitnick & Simon, 2002). Accordingly, phishing emails and messages often exploit this trust by pretending to be originated from trusted sources, such as friends, government agencies like the Internal Revenue Service, or service providers like banks or credit card companies.

As a critical component of the modern computing systems, humans create most persistent security vulnerabilities as they control system designs and configurations as well as input and output and make decisions on whether or not to click malicious links in phishing emails (Wash & Cooper, 2018). Research on human psychology indicates that online phishing has been gaining popularity due to the flaw in hu-

Table 1. Industries targeted by phishing

Industries	Percentage
Email/Online Services	26.1%
Financial Institutions	20.5%
Payment Services	16.1%
Cloud Storage/File Hosting	13.8%
E-Commerce	7.6%
Software-as-a-Service (SaaS)	7.1%
Social Networking	4.5%
Dating	0.9%
Government Services	0.5%
Other	3.0%

Source: PhishLabs, 2018

man susceptibility (Kleitman, Law, & Kay, 2018). Recognizing the weak human link, cyber criminals have moved toward increased use of social engineering attacks. The Human Factor report finds that cyber criminals have relied less on the use of indiscriminate automated attack while increasing the use of social engineering with more success and impact through highly personalized spear-phishing campaigns targeting specific individuals (Proofpoint, 2017). As evidence of the effectiveness and impact of the human-driven phishing exploits, the report finds that 99% of email-based financial fraud attacks depended on human user clicks on the spear phishing URLs instead of automated exploits for malware installation and that almost 90% of the clicks on the malicious phishing links took place within 24 hours of email delivery (Proofpoint, 2017).

Online phishing via social engineering is a leading cause for identity theft for individual consumers, and about 7% of individuals age 16 and older in the United States were victims of identity theft (U.S. Department of Justice, 2017). In addition, online criminals have been increasingly targeting enterprise organizations by impersonating services such as email service providers and Software as a Service (SaaS) platforms to access and steal corporate data. The latest 2018 Phishing Trends and Intelligence Report shows that phishing continues to be the top threat for cyberattacks and that social engineering to exploit human vulnerabilities continues to be the leading and most successful method of phishing attacks (PhishLabs, 2018). Table 1 below shows the industries targeted by phishing based on the findings from the report by PhishLabs (2018). The report also finds that the total number of phishing attacks went up by two percent in 2017 and that these five industries were the target of over 84% of all phishing attacks in 2017: email/online services, financial institutions, payment services, cloud storage/file hosting services, and e-commerce companies (PhishLabs, 2018).

The trends and techniques in online phishing are dynamic and may provide insight on the how and why the victims and organizations are targeted. Table 2 below shows the major changes and trends in phishing volume based on the findings from the report by PhishLabs (2018).

The data in both Table 1 and Table 2 above indicate that online phishers continue to target corporate organizations, such as email/online services and financial institutions probably for maximum profit. Phishing attacks targeting Software-as-a-Service (SaaS) and Social Networking soared with growths of 237% and 190% respectively. The exceptional increases in phishing attacks on SaaS, such as Adobe and DocuSign, is less about gaining access to the SaaS services but more about using the trustworthi-

Table 2. Changes in phishing volume

Industries	Percentage of Increase (+)	Industries	Percentage of Decrease (-)
Software-as-a-Service	+237%	Financial Institutions	-11%
Social Networking	+190%	E-Commerce	-32%
Telecommunications	+67%	Cloud Storage/File Hosting	-40%
Shipping Services	+30%	Dating	-44%
Email/Online Services	+26%	Government Services	-70%
Payment Services	+14%		

Source: PhishLabs, 2018

ness of the SaaS brands to social engineer victims into giving up their email credentials (PhishLabs, 2018). Social media platforms may allow creation of fake identities and provide opportunities for social engineering attacks and obtaining sensitive personal information (Krombholz, Hobel, Huber, & Weippl, 2015). Social media sites may also be used as a trusted source to lure phishing victims to malicious files and links (Nelson, Lin, Chen, Iglesias, & Li, 2016). The fast growing phishing attacks targeting social media platforms can be attributed to the established trust relationship between users and the platform that could be used by attackers for social engineering to facilitate additional online crime (PhishLabs, 2018).

Using established trust is essential to social engineering for online phishing attacks. Phishing emails and fraudulent websites may employ a variety of technical subterfuge or visual similarity tricks to make them look like trusted or legitimate sources (Gupta, Arachchilage, & Psannis, 2018; Heartfield & Loukas, 2015; Krombholz, Hobel, Huber, & Weippl, 2015; Nelson, Lin, Chen, Iglesias, & Li, 2016). There was a recent surge in the use of the secure HTTPS protocol and free SSL certificates in online phishing sites (PhishLabs, 2018). As consumers are trained to recognize HTTPS as a security indicator for trustworthy websites, online phishers are using the HTTPS protocol to exploit consumers' trust for the protocol and trick them into surrendering sensitive personal information or downloading malware. Ironically, the encryption and security mechanism commonly used for secure online transactions is used by online phishers against consumers. Statistically, there has been a fast increase in the number of phishing sites using the HTTPS feature. The latest trend report by the Anti-Phishing Working Group (APWG) shows that 35 percent of phishing attacks were hosted on Websites using HTTPS and SSL certificates by the second quarter of 2018 compared with only less than five percent of phishing sites using HTTPS and SSL at the end of 2016 (APWG, 2018).

Theoretically, psychological principles of persuasion are the key to understanding how online phishers use social engineering techniques to manipulate phishing victims and exploit their trust. The anatomy of successful social engineering attacks by Bullée et al. (2018) has identified six persuasion principles often used in social engineering attacks. Table 3 below presents the six principles of persuasion, brief illustrations with examples, and their respective percentage of occurrence in social engineering attacks in the order of occurrence from the highest to the lowest.

Each actual social engineering attack may use one or more of the persuasion principles along with other technical or social techniques to deceive the victims of phishing. In reality, there are a wide variety of online phishing types based on their targets and techniques. The following sections will classify and discuss the types of phishing and propose a comprehensive set of solutions.

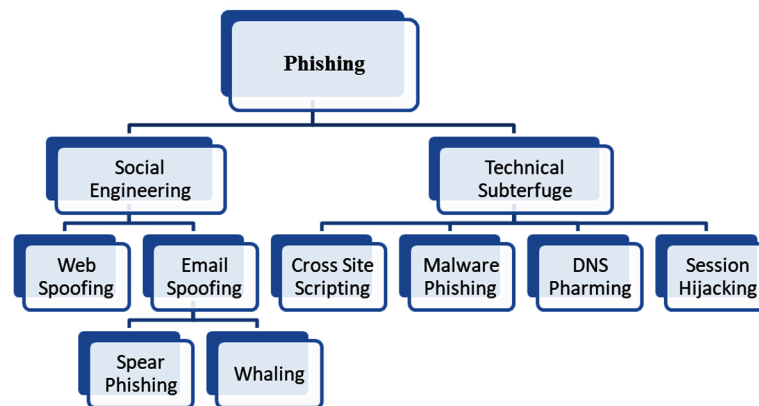
Table 3. Persuasion principles used in social engineering attacks

Persuasion Principle	Brief Illustration	Occurrence
Authority	The phisher claims that he is from the security department and needs the target's username and password for security updates.	63.3%
Liking	The phisher claims similar background or personal interest to establish rapport and trust with the target.	13.3%
Reciprocity	The phisher claims that he needs the target's login credentials to help solve a real or made-up technical problem for the target.	11.1%
Commitment	The phisher approaches the target multiple times and obtains sensitive information from the target incrementally.	10.6%
Conformity	The phisher claims that the target's peers have provided what he needs in a survey and that the target should do the same.	1.1%
Scarcity	The phisher claims a limited-time offer for online registration to lure and trick the target to register online at the phishing website.	0.6%

Source: Bullée et al., 2018

Figure 1. Adapted taxonomy of phishing attacks

Source: Gupta, Arachchilage, & Psannis, 2018



TYPES OF ONLINE PHISHING

In terms of mechanisms and techniques used, online phishing can be classified into two general categories or types, Social Engineering and Technical Subterfuge, and multiple sub-types under each category. Such a classification of phishing is illustrated in Figure 1 below adapted from the taxonomy by Gupta, Arachchilage, and Psannis (2018). The types and sub-types in the taxonomy only reflect a relative emphasis and weight between social engineering methods and mechanisms of technical subterfuge as actual phishing attacks may employ a mixture of various methods and techniques.

SOCIAL ENGINEERING

Email Spoofing

The predominate types of phishing using social engineering schemes are email spoofing and web spoofing, or fake websites. Email spoofing may occur in spear phishing or whaling. Spear phishing is the most common and most effective type of phishing, which was the starting point for 91% of successful cyberattacks and the resulting data breach (PhishMe, 2016). Spear phishing uses personalized emails containing malicious attachments or fraudulent web links to target specific members or groups of an organization. Spear phishing attackers often conduct social engineering research about the target to make the phishing emails appear legitimate and from a trusted source (Nelson et al., 2016). Examples of spear phishing include a fake email message that appears to come from your human resources department asking you to click a link to log in to view, download, and print important documents like paystubs and W-2 tax document, or a message seemingly from a technical service company asking you to sign a service contract attached (UC Berkeley, 2018). Such messages are appealing and deceptive to individuals as they use specific and personalized issues of concern and look like coming from the community close to your work or life. Victims who click and open the fraudulent and malicious links or attachments in such phishing emails may have their login credentials or sensitive financial information stolen or have malware, such as ransomware, downloaded and installed on their systems. Whaling is a special type of spear phishing that targets high-rank individuals such as executives of an organization, who may have privileged possession of or access to sensitive data.

Web Spoofing

Web spoofing is using fake websites to phish and trick users into giving up their personal information. A phisher could forge a website that appears identical to an authentic website to mislead the user to enter personal information to be collected by the attacker (Banu & Banu, 2013). A major website spoofing trick is to manipulate the link tag and content to make the web link display an authentic URL whereas it is directed to a fake and malicious URL in the background (Varshney, Misra, & Atrey, 2016). Web spoofing is often combined with email spoofing with the link to the fake website embedded in the phishing email (Gupta, Arachchilage, & Psannis, 2018). For example, a phishing email may include a logo that looks very close or identical to the company logo on PayPal's website and a link to update one's PayPal account information that goes to a nefarious website (UC Berkeley, 2018).

Technical Subterfuge

Cross Site Scripting

Cross site scripting (XSS) is a common web security vulnerability that allows an attacker to inject HTML tags and malicious JavaScript code into the dynamic web page displayed in the victim's web browser where the cookies containing login credentials and session information can be stolen by the attacker (Gupta & Sharma, 2012). There are two main types of server-side XSS attacks: (1) Persistent XSS attacks in which the code injection is permanently stored in the server and affects the subsequent users visiting the web page; and (2) Non-persistent or reflected XSS is the most common type of XSS attack where the code injection is not permanently stored on the server but immediately displayed and executed

by the victim's web browser if the victim clicks on the malicious URL (Manaa & Hussein, 2016). The XSS attacks are technically crafted, but social engineering techniques may also be used by phishers to lure victims to click the malicious web links. The injection of malicious code into web applications is due to the lack of filtering and authentication of web input (Gupta, Arachchilage, & Psannis, 2018).

Malware Phishing

Malware phishing installs malicious software onto the victim's computer, collects sensitive information from the victim and sends it back to the phisher (Gupta, Arachchilage, & Psannis, 2018). Malware used in online phishing includes viruses, worms, Trojan horses, spyware, rootkits, and key loggers. The malware that targets victims often comes in mobile code from webpage download that includes potentially malicious executable code along with text, images, audio, and video. The malware installation is often stealthy without the victim's awareness or consent. Social engineering phishing techniques, such as lucrative offers of free downloads, free trips, and prizes, may also be used to lure the victims to the malware websites.

DNS Pharming

DNS (Domain Name Systems) pharming aims to direct the victim to visit a malicious website by providing a fraudulent mapping of the IP address and the domain name requested by the victim. In a DNS pharming attack, the phisher may set up a fake DNS server for victims to connect to. Alternatively, DNS cache poisoning may be used by phishers to respond and feed local DNS cache resolver with incorrect records and fraudulent IP address pointing to a malicious URL (Banu & Banu, 2013). DNS pharming does not depend on social engineering techniques as it poisons the domain-IP mapping without the victim's awareness or active participation.

Session Hijacking

Session hijacking uses IP address spoofing and Man-in-the-Middle tricks to impersonate a legitimate host, such as a client or server in a network connection and allows the attacker to monitor, eavesdrop, and hijack the network communication and change, delete, modify, forge, and even redirect data to the attacker's intended destination (Whitman & Mattord, 2019). The attacker may also hijack the session key, often in the wireless LAN connections, to steal user credentials for illicit access to data (Gupta, Arachchilage, & Psannis, 2018). Theft of user credentials and sensitive data via session hijacking is a type of digital and technical impersonation without the victim's knowledge.

SOLUTIONS AND RECOMMENDATIONS

Online phishing threats involve both social engineering tricks and technical deceptions that exploit human vulnerabilities and lack of awareness and protection. Therefore, this article proposes a comprehensive set of solutions and recommendations to prevent, detect, mitigate, and defend against online phishing attacks. The proposed solutions consist of anti-phishing awareness education and training and technical controls.

Awareness Education and Training

It is a general consensus in the anti-phishing research community that awareness training and education is the most important solution to improve human judgement and behavior to mitigate and prevent the risks of online phishing attacks. Education is a critical component in the defense-in-depth security model, and user awareness training can lower user susceptibility to deceptive phishing attacks that target human vulnerabilities (Hearfield & Loukas, 2015). Anti-phishing training and education programs and events should be offered on a regular basis by schools, businesses, and government and public services to inform and alert students, consumers, employees, and the public about the risks of social engineering tricks and online phishing attacks and corresponding methods and tools of detection and prevention. The topics and delivery methods may be customized according to organizational and business needs to maximize the effectiveness. Online vendors can help with user awareness training by providing useful anti-phishing cues and messages to educate and remind users about web phishing risks and on how to verify target URLs and security indicators such as the https protocol, pad lock icon, digital certificate, as well as security and encryption standards used for mobile sites, including WPA2 (WiFi Protected Access II) and AES (Advanced Encryption Standard).

Established information security policies, processes, procedures and guidelines should be regularly updated and integrated with user awareness training and organizational communication to strengthen the human factor to defend against social engineering attacks such as phishing (Heartfield & Loukas, 2015; Mitnick & Simon, 2002). Organizational anti-phishing awareness training should include clear communications on phishing related security updates, policies, and procedures. Security policy communication and updates should include regular reminders of user password expiration and updates, adoption of multi-factor authentication for stronger security and user account protection, and DLP (data loss prevention) education to avoid sensitive information in unencrypted emails. In addition, organizations should make users aware of standard internal and external reporting procedures and resources in case of being a victim of online phishing. For example, consumers can report phishing emails to the Anti-Phishing Working Group (APWG) by email at reportphishing@apwg.org and victims of online phishing and identity theft in the U.S. may file a report with the Federal Trade Commission online at <https://www.ftc.gov/complaint>.

A valuable public resource for anti-phishing education and awareness training is the free and up-to-date phishing alerts and advisories published by the United States Computer Emergency Readiness Team (US-CERT). US-CERT also provides important tips on avoiding social engineering and phishing attacks, which include the following best practices for online users to avoid falling a victim of phishing (US-CERT, 2018):

- Be suspicious of unsolicited phone calls, visits, or emails from unknown individuals asking about employees or other internal information.
- Do not provide personal or organizational information to persons of unknown identity.
- Do not respond to email solicitations or click links in emails asking for personal or financial information.
- Do not submit sensitive information online before verifying the website's URL and security.
- Install and maintain anti-virus software, firewalls, and email filters to reduce phishing email traffic and use anti-phishing features offered by your email client and web browser.

A special type of phishing awareness education and training is needed to prevent and mitigate phishing risks for elderly users who are especially vulnerable to phishing attacks (Lee, 2018). According to the FBI 2017 Internet crime report, the total financial losses from online crimes reached \$1.42 billion and those over 60 years old ranked the highest in the total number of victims and the total amount of financial loss (FBI, 2018). More interactive training on the safe use of digital media, online privacy protection, and defense techniques against email and web phishing should be made available to elderly consumers on a regular basis at community centers, public libraries, and senior living facilities.

Technical Controls

Awareness education and training solutions proposed above are of primary significance as they will improve user behavior and judgment in defending against social engineering and online phishing from the client side. Technical solutions, such as implementations of technical controls on the server side, are also necessary to help to prevent, detect, and mitigate phishing risks in the online environment. The following are important recommendations for server side technical solutions to online phishing.

Server side filtering and authentication technology can be used to detect and prevent email phishing. Email filtering includes: (1) Anti-spam filtering used for verifying email origins and other sender details to filter out substantial amount of malicious email traffic; and (2) DNS-based blacklisting to profile, detect, and block traffic from blacklisted sources (Gupta, Arachchilage, & Psannis, 2018). More importantly, mail server authentication technology should be used by the receiving mail server to validate the source IP address of sending server before potential phishing email traffic reaches the target users. In addition, organizations with frequent needs for data loss prevention in emails should consider digitally signing emails. Receiving e-mail servers can be configured to check and validate digitally signed inbound emails and alert recipients of unsigned or invalid emails, and out-bound emails can also be signed with an official corporate digital certificate to assure the recipients of the authenticity and legitimacy of the email (Ollmann, 2017).

Furthermore, DNS-based authentication also helps to block illegitimate domains and mitigate the negative effect of DNS poisoning or pharming. Implementation of Domain Name System Security Extensions (DNSSEC) and its regular updates are also recommended to defend against DNS pharming as DNSSEC provides origin authentication and integrity check of DNS records. With DNSSEC, the resolvers can verify if the data for the DNS query exists or not, if the existing data is from a reliable source and if it has been modified.

Active web monitoring is a useful solution to combating the most challenging type of web spoofing that targets victims with visual similarities. Visual similarity based phishing detection is an example of active web monitoring that checks for similar web pages and user data and generates a warning upon detection of similar web pages asking for the same sensitive information (Gupta, Arachchilage, & Psannis, 2018). Technically, managed service providers may use agent-based bots to monitor URLs and web content remotely and detect unauthorized use of a company's unique logo, trademark and web content against the legitimate company profile and authorized users of the company web resources (Ollmann, 2017).

Web phishing via cross site scripting (XSS) can be technically prevented by web input validation to stop malicious code injection. Client side web browser solutions may degrade the client system performance and web surfing experience (Gupta & Sharma, 2012). XSS attacks are often successful and undetectable to client-side protection strategies because of inherent trust relationships between the user and the website owner (Ollmann, 2017). Therefore, securing web applications with robust content check and input validation on the server side is the best solution to protect consumers from XSS phishing attacks.

The anti-phishing guide from the IBM Internet Security Systems offers the following best practices and guidelines for implementing successful content validation (Ollmann, 2017):

- Never trust data submitted by a user or other application components.
- Always sanitize user submitted data before processing or storing it or giving it to an application user.
- All data must be sanitized by decoding common encoding schemes back to their root character to avoid any unsafe characters used for attempted code injection.
- Replace all harmful HTML web language characters with safe versions to prevent attempted executable code injections using the harmful HTML characters.

To prevent online phishing using Man-in-the-Middle (MIMT) attacks and session hijacking, application providers and developers should avoid accepting session information within a URL, implement timeout and integrity checks for the SessionID for each client request, and revoke and replace expired and invalid SessionIDs (Ollmann, 2017). Additionally, organizations should require or recommend the use of VPN (virtual private network) connections, proxy server with data encryption, and secure shell (SSH) for remote connections to prevent MIMT attacks and session hijacking (Chandel, Kumar, & Yadav, 2017).

Malware phishing often succeeds through user download of malicious software from websites or email attachments. Awareness education and training is critical to the prevention of malware phishing. However, some technical and security implementations at the organization level are helpful solutions as well. For example, Microsoft Office Macros are still the top means of malware delivery as the Microsoft Office macro feature is usually enabled by default (Zurkus, 2018). Moving applications, such as Microsoft Office applications, from local installations to the cloud can provide centralized and more secure control and management of application installation, updates and data management. In addition, regular implementations and use of firewalls, malware scans, and intrusion detection and prevention systems will help prevent and minimize malware phishing attacks.

FUTURE RESEARCH DIRECTIONS

Phishing continues to be a common method for exploiting human vulnerabilities in cyber attacks today, and it remains an important challenge to train users to recognize and avoid clicking malicious links in phishing emails (Wash & Cooper, 2018). The latest state of phishing report confirms that there has been a steady increase in the volume of phishing attacks and that security awareness education and training has become the most important factor in assessing end user security risks to organizations (Wombat Security, 2018). Future research on phishing awareness education and training needs to focus more on how to innovate curricula and delivery methods for training and on how to assess the effectiveness of training. There should also be more research on how to better understand and protect senior citizens in particular, who are especially vulnerable to online phishing.

With fast growing Internet of Things (IoT) devices and connections, IoT security research needs to address IoT phishing risks and defense mechanisms. As IoT security is still weak, hackers are able to use thingbots, or botnets of infected IoT devices, to relay malicious emails without resorting to malware (Gupta, Arachchilage, & Psannis, 2018). Therefore, how to prevent phishing with IoT devices will be an interesting and important challenge for future research.

CONCLUSION

This article introduces and defines online phishing, which is an online crime of deceiving users into accessing fraudulent emails, web links and websites to steal their sensitive private information. Online phishing is the top starting point for cyberattacks and the leading cause for identity theft that brings financial and other losses to individual and organizational victims. Phishing is primarily a social engineering attack that exploits human vulnerabilities due to lack of user awareness and protection. This article classifies phishing into two groups based on the primary method and technique involved: Social Engineering and Technical Subterfuge. The social engineering group includes web spoofing and email spoofing. Technical deceptions include cross site scripting, malware phishing, DNS pharming, and session hijacking. The primary solution to combating online phishing should be user awareness education and training to improve human behavior and judgment in order to minimize the occurrence of phishing victims. Technical solutions, best practices, and guidelines are also offered in this article to help create a more secure environment to prevent and detect online phishing. This article recognizes that there are significant questions and challenges for future research on phishing, such as on how to design, deliver and assess effective phishing awareness education and training and how to combat and prevent phishing in the emerging IoT environment.

REFERENCES

- Alexander, M. (2016). Methods for Understanding and Reducing Social Engineering Attacks. Retrieved from <https://www.sans.org/reading-room/whitepapers/critical/paper/36972>
- Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., & Savage, S. (2012). Measuring the cost of cybercrime. *Proceedings of Workshop on Economics of Information Security (WEIS 2012)*, 1-31.
- APWG (Anti-phishing Working Group). (2018). Phishing Activity Trends Report, 2nd Quarter 2018. Retrieved from <https://www.apwg.org/resources/apwg-reports/>
- Banu, M. Z., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies*, 4(6), 783–786.
- Bullée, J. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks – A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, 15(1), 20–45. doi:10.1002/jip.1482
- Chandel, A., Kumar, P., & Yadav, D. K. (2017). Phishing attacks and countermeasures. *International Journals of Advanced Research in Computer Science and Software Engineering*, 7(6), 246–253. doi:10.23956/ijarcsse/V7I6/0227
- Chen, Y., YeckehZaare, I., & Zhang, A.F. (2018). Real or bogus: Predicting susceptibility to phishing with economic experiments. *PLoS One*, 13(6). doi:10.1371/journal.pone.0198213
- FBI. (2018). 2017 Internet Crime Report. Retrieved from https://pdf.ic3.gov/2017_ic3report.pdf

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247–267. doi:10.1007/11235-017-0334-z

Gupta, S., & Sharma, L. (2012). Exploitation of cross-site scripting (XSS) vulnerability on real world web applications and its defense. *International Journal of Computers and Applications*, 60(14), 28–33. doi:10.5120/9762-3594

Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, 48(3), 1–39.

Kleitman, S., Law, M. K. H., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. [PubMed]. *PLoS One*, 13(10), e0205089. doi:10.1371/journal.pone.0205089

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015, June). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. doi:10.1016/j.jisa.2014.09.005

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(9), 1–10.

Manaa, M. E., & Hussein, R. (2016). Preventing cross site scripting attacks in websites. *Asian Journal of Information Technology*, 15(16), 2797–2804.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. John Wiley & Sons, Inc.

Nelson, J., Lin, X., Chen, C., Iglesias, J., & Li, J. J. (2016). *Social engineering for security attacks. MISNC, SI, DS '16*. NJ: Union; doi:10.1145/2955129.2955158

Ollmann, G. (2017). The Phishing Guide: Understanding & Preventing Phishing Attacks. Retrieved from <http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf>

PhishLabs. (2018). 2018 Phishing Trends & Intelligence Report: Hacking the Human. Retrieved from www.phishlabs.com

PhishMe. (2016). 2016 Phishing Susceptibility and Resiliency Report. Retrieved from www.phishme.com

Ponemon Institute. (2017). 2017 Cost of data breach study. Retrieved from <https://www.ibm.com/security/data-breach>

Proofpoint. (2017). The Human Factor 2017. Retrieved from <https://www.proofpoint.com/sites/default/files/pfpt-en-uk-human-factor-report-2017.pdf>

Berkeley, U. C. (2018). Phishing Examples Archive. Retrieved from <https://security.berkeley.edu/resources/phishing/phishing-examples-archive>

US-CERT. (2018). Avoiding Social Engineering and Phishing Attacks. Retrieved from <https://www.us-cert.gov/ncas/tips/ST04-014>

U.S. Department of Justice. (2017). Victims of Identity Theft. Retrieved from <https://www.bjs.gov/content/pub/pdf/vit14.pdf>

Varshney, G., Misra, M., & Atrey, P. K. (2016). A survey and classification of web phishing detection schemes. *Security and Communication Networks*, 9(18), 6266–6284. doi:10.1002/ec.1674

Verizon. (2018). 2018 data breach investigations report (11th ed.). Retrieved from <http://www.verizonenterprise.com/>

Wash, R., & Cooper, M. M. (2018). Who provides phishing training? Facts, stories, and people like me. CHI 2018, Montréal, Canada. Doi:10.1145/3173574.3174066

Whitman, M. E., & Mattord, H. J. (2019). *Management of information security* (6th ed.). Boston, MA: Cengage.

Wombat Security. (2015). The Cost of Phishing & Value of Employee Training. Retrieved from <https://www.wombatsecurity.com/cost-of-phishing>

Wombat Security. (2016). The State of the Phish. Retrieved from <https://www.wombatsecurity.com/state-of-the-phish>

Zurkus, K. (2018, September 14). Microsoft Office Macros Still No. 1 Malware Delivery. Retrieved from <https://www.infosecurity-magazine.com/news/microsoft-office-macros-still-no-1/>

ADDITIONAL READING

Bossetta, M. (2018). The weaponization of social media: Spear phishing and cyberattacks on democracy. *Journal of International Affairs*, 71(1), 97–106.

Boyle, R. J., & Panko, R. (2015). *Corporate computer security* (4th ed.). Upper Saddle River, NJ: Pearson Education Inc.

Ciampa, M. (2018). *Security+ Guide to Network Security Fundamentals* (6th ed.). Boston, MA: Cengage.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing & Applications*, 28(12), 3629–3654. doi:10.1007/00521-016-2275-y

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91.

Martin, J., Dube, C., & Coover, M. D. (2018). Signal Detection Theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks. [PubMed]. *Human Factors*, 60(8), 1179–1191. doi:10.1177/0018720818789818

Resnik, D. B., & Finn, P. R. (2018). Ethics and phishing experiments. [PubMed]. *Science and Engineering Ethics*, 24(4), 1241–1252. doi:10.1007/11948-017-9952-9

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 17(11), 759–783. doi:10.17705/1jais.00442

KEY TERMS AND DEFINITIONS

Cross-Site Scripting (XSS): Injecting malicious code to be displayed in the victim's web browser to steal the victim's credentials.

DNS Pharming: Providing a fraudulent DNS mapping to direct a victim to visit a fake and malicious website.

Identity Theft: The crime of stealing sensitive personal information, such as usernames, passwords, date of birth, social security number, and personal and financial information.

Online Phishing: An online criminal attempt via fraudulent emails, web links, and websites to trick online users to surrender sensitive private information.

Session Hijacking: Using a spoofed IP address or Man-in-the Middle techniques to impersonate a legitimate host to eavesdrop or redirect network communication.

Social Engineering: An attack that uses personal and social skills to persuade the target to behave in violation of security principles.

Spear Phishing: Phishing for sensitive information by using personalized emails containing malicious attachments or fraudulent web links to target specific members or groups of an organization.

Technical Subterfuge: The act of deceiving victims and stealing their sensitive information by technical means.

Web Spoofing: Using fake websites to phish and trick users into giving up their personal information.

Whaling: A special type of spear phishing that targets high-rank individuals such as executives of an organization.

Crime Hidden in Email Spam

4

Szde Yu

Wichita State University, USA

INTRODUCTION

Crime on the web has gained significant attention in recent years. In the past, the study of cybercrime was not exactly new but it was by no means a focal concern in the mainstream criminology. Nowadays, however, it seems every crime could have a cyber-related component in it and therefore potentially all crimes can be committed or facilitated by the use of cyberspace. For example, even though you still cannot murder or rape someone on the Internet, you could stalk your victim on the Internet beforehand or you could video-record the crime and sell the footage in the black market. Typically such online black markets exist on the so-called Dark Web or Deep Web. On the Dark Web, you can advertise anything you have to offer or you might find anything you need with a price. Conceivably many things happening on the Dark Web are not legal. Otherwise, they could have simply done the transaction on Amazon.com. In other chapters, the definition of the Dark Web has been provided and how it functions has been discussed. Instead of repeating them, this chapter focuses on how information is being disseminated in the cyber-criminal-world since criminal activities on the Dark Web cannot be Googled. More precisely, the focus is on email spam and the role it plays in facilitating criminal activities that may or may not necessarily take place on the Dark Web. Email spam has long been dismissed as a trivial crime that does not usually warrant much attention from either academics or practitioners. Nonetheless, its low-profile status among crimes may have actually endowed email spam with the best utility in criminal communication.

BACKGROUND

Email spam is defined as unsolicited commercial electronic mail that includes any commercial emails addressed to a recipient with whom the sender has no existing business or personal relationship and not sent with the consent of the recipient, and commercial electronic mail is defined as any electronic mail message the primary purpose of which is commercial advertisement or promotion of products or service (Rogers, 2006). Sending spam emails can be treated as a criminal offense in the United States, according to the CAN-SPAM Act enacted in 2003. The Act imposes penalties on sending unsolicited commercial email if the provisions set by the Act are violated. The Federal Trade Commission (FTC) is in charge of enforcement of these provisions and it also provides regulations of which any violation can be declared criminal (FTC, 2009). The FTC regulations are as follows: 1. Don't use false or misleading header information; 2. Don't use deceptive subject lines; 3. Identify the message as an ad; 4. Tell recipients how to opt out and honor opt-out promptly; 5. Monitor what others are doing on your behalf (FTC, 2009). In 2008, the so-called "Spam King" Robert Soloway was convicted under the CAN-SPAM Act and was sentenced to 47 months in federal prison (Rabinovitch, 2007). The Act also allows states and Internet service providers to file civil lawsuits against spammers (Ford, 2005; Yeargain et al., 2004). Despite this, email spam has never been seen as a serious crime even though email spam is probably one of the most

DOI: 10.4018/978-1-5225-9715-5.ch057

prevalent crimes as almost every person who uses email has received at least some unsolicited junk emails that aim at advertising, phishing or scamming. Most people tend to simply delete them or rely on the spam filter embedded by the service provider to screen them out. However, spam filters are not entirely reliable. As a result, users often have to check the spam folder to see if some important messages have been mistakenly flagged as spam (i.e., false positive). A false positive could cost a delay or omission in an important communication and sometimes this could entail significant consequences (Weinstein, 2003). Therefore, it is an understatement to say email spam is nothing more than a nuisance. In fact, email spam can be costly. Some research has indicated that the time and productivity wasted on account of email spam can amount to 20 billion dollars every year (Yeargain, et al., 2004). The energy used to transmit, process, and filter spam can be equivalent to the electricity used in 2.4 million households annually (McAfee, 2009). In addition, the cost of email spam can be much higher when it is being utilized as a communicative avenue for criminal purposes, such as scam, illicit drug selling, and sex crimes (Yu, 2015a). Unfortunately, the link between email spam and other crimes has long been overlooked. Accordingly, in this chapter the criminal activities associated with email spam are discussed regarding how email spam is being used by criminals to reach potential customers and victims.

FOCUS OF THE ARTICLE

Scam/Fraud

Money is a common motive behind a variety of crimes and email spam is one of these crimes. While many spammers send advertisements to promote commercial products, some spammers resort to scam or fraud. Some scam schemes are elaborate while others could seemingly lack sophistication. Many people are familiar with that Nigerian prince who is looking for someone to help him move money around, and he allegedly is so grateful that he is willing to pay the helper a whopping proportion of his fortune. In addition, many people are lucky enough to have won a lottery they do not remember buying, but no matter how big the winning prize is the lucky winner somehow is always asked to pay a processing fee first. Lately, scammers seem to prefer impersonation. They might pretend to be the IT department in your organization and ask for your passwords, or they could pretend to be your bank and ask for your account information. These schemes are getting old but at least the scammer is willing to make up a story. Some schemes are simply carried out in an email that has only one or two sentences, such as “you have a message; click here.” However, they could work as well thanks to people’s curiosity. Phishing is a very popular way of luring people to visit a website where the actual scam will take place so that the scammer does not need to disclose too much in the email. This method also allows scammers to remain hard to trace by using a false sender address or changing servers, because they do not need to wait for your reply. If they need to wait for the recipient to reply like the Nigerian prince usually would, it means the scammers have to stay active on the same email server for a while, which increases the odds of being caught.

Regardless of the scheme being used, in essence scammers are trying to acquire sensitive personal information so that they can either use it directly or sell it for profit. Figure 1 is an example of scam email. It is typical for scammers to try to establish contact by implying you are the chosen one but they cannot really address you by your name because this identical email was sent to possibly hundreds or even thousands of people at the same time, which is characteristic of email spam. This is especially true in the past when spammers mostly rely on a web crawler to collect email addresses randomly from

Figure 1.

From: CENTRAL BANK OF NIGERIA <telx@centralbkng.org>
 Date: 2000/1/2
 Subject: OVERDUE CONTRACT/INHERITANCE PAYMENT
 To:

ATTN: BENEFICIARY.

THIS IS TO OFFICIALLY NOTIFY YOU THAT YOUR OVERDUE CONTRACT FUNDS HAS FINALLY BEEN APPROVED FOR IMMEDIATE PAYMENT BY THE NEW PRESIDENT HIS EXCELLENCY GOODLUCK JOHNSON (GOON) VIA MY ESTEEM OFFICE AS THE CHANCELLER GENERAL FEDERAL REPUBLIC OF NIGERIA (FRN). AS A MATTER OF URGENCY NOW, I HAVE ALREADY DUSTED YOUR FILE SINCE LAST WEEK BEFORE I DEEMED IT FIT TO CONTACT YOU IN REGARDING TO THIS DEVELOPMENT IN FAVOR OF OUR DEAR UNPAID FOREIGN CONTRACTORS WHO EXECUTED CONTRACT GENUINELY WITH OUR DEAR GOVERNMENT BUT STILL REMAIN UNEARD DUE TO THEIR DEALING WITH SOME FAKE OFFICERS WHO ARE IMPERSONATING SOME TOP OFFICERS IN GOVERNMENT BY USING FORGED LETTER HEADED PAPERS AND OTHER FEDERAL GOVERNMENT RELATED DOCUMENTS TO PRACTICE FRAUD THROUGH DIFFERENT MEANS.

IN VIEW OF THIS NOW, A TOTAL SUM OF USD 10,000,000.00 (TEN MILLION UNITED STATES DOLLARS) ONLY, HAS BEEN APPROVED TO BE PAID TO YOU IN THIS FIRST QUOTA VIA INTERNATIONAL WIRE TRANSFER ISSUED IN CARE OF FIRST BANK OF NIGERIA PLC AND YOUR BALANCE WILL COME UP IN THE NEXT QUOTA. BE OFFICIALLY AWARE THAT THIS DEVELOPMENT CAME UP LATE LAST WEEK AFTER OUR CLOSE DOOR MEETING WITH NATIONAL HOUSE OF ASSEMBLY MEMBERS IN CONJUNCTION WITH THE SENATE PRESIDENT (SENATOR DAVID MARK) CONTACT MR. JOHN ABON (DIR. TELEX DEPT) ON HIS OPEN ACCESS EMAIL BELOW:
 EMAIL: firstbanktelxdept@gmail.com
 Tel: +234-7090933118

AND YOU ARE ADVISED TO FURNISH ME WITH YOUR BANKING INFORMATION AND CONTRACT DETAILS WHICH PROOFS THE GENUINITY AND AUTHENTICATION OF YOUR FUNDS AS A GENUINE CONTRACTOR WITH FEDERAL GOVERNMENT OF NIGERIA (FGN). ALSO YOU ARE REQUESTED TO SEND ACROSS YOUR INTERNATIONAL PASSPORT PHOTOGRAPH OR YOUR DRIVERS LICENCE BEFORE WE CAN CARRY ON THIS EXERCISE WITHOUT FURTHER DELAY.

AND SECURITY REPORT REACHING MY DESK STATED THAT YOU ARE STILL DEALING WITH SOME FRAUDSTERS HERE IN NIGERIA WHO ARE IMPERSONATING MY PERSON AS THE CHANCELLER GENERAL OF THE FEDERATION (CGF) WITHOUT PORTFOLIO BE WARNED TO AVOID PUTTING YOURSELF INTO PROBLEMS AND AS A RESULT OF MUCKING YOU THROUGH FRAUDULENT MEANS.

WE WARNED YOU SHOULD DESIST FROM ANY OTHER AGENCIES RELATED TO YOUR FUNDS LOCAL OR INTERNATIONAL BECAUSE ALL ARRANGEMENT THAT HAS BEEN CANCELLED SINCE LAST WEEK AND THE MANDATE GIVEN TO ACCOUNTANT GENERAL OF THE FEDERATION (AGF) WORLD BANK AUDITORS (WBA) HAS BEEN WITHDRAWN SINCE LAST WEEK DUE TO THEIR INABILITY TO CARRY ON THE EXERCISE AND THEIR ATTEMPT PUTTING OUR DEAR FOREIGN CONTRACTORS INTO FINANCIAL DIFFICULTIES. I WILL LIKE YOU TO CALL ME TODAY ON MY HOTLINE +234-7091236462 FOR MORE DETAILS AND TO YOUR PAYMENT UPDATE. ON BEHALF OF THE FEDERAL GOVERNMENT OF NIGERIA (FGN) WE APOLOGISE FOR YOUR GREAT LOSS AND UGLY EXPERIENCE IN THE PAST.

AWAITING YOUR URGENT CALL.

CONGRATULATIONS AT LAST.

BEST REGARDS,

MR. DAVID SMITH
 DIRECTOR, TELEX DEPT CBN

various webpages. Nowadays, however, more and more spammers acquire a list of email addresses from data stolen from systematic sources, such as the members of popular social media sites or customer information from a bank. This allows them to link each email address to a name or even a social security number in some cases. Therefore, a sophisticated scam email might start by addressing your name correctly and lead you to believe this is an authentic personal email, while in actuality the same email was still sent to a long list of recipients with each person's name customized. It is noteworthy that some scam attempts are indeed personal. It follows that the scammer is targeting you per se instead of a list of random people on the Internet, but this tactic is outside the realm of email spam as sending a personal email does not fit the definition of spam.

Using email spam as the communicative avenue provides two major benefits for scammers. First, it allows scammers to reach a wide range of potential victims. Granted, most people do not take these emails seriously, but the odds of someone actually taking the bait will increase when the scam email can reach more people. Greed and curiosity are the two human elements that scammers are counting on no matter how elaborate or simplistic their scheme might seem (Yu, 2011). Second, hiding scam inside spam provides protection for scammers. One standalone email attempting to steal your money could appear alarming or even threatening to many people, but if it shows up in a mix of unsolicited emails, most people would dismiss it as just another junk email. Such dismissal reduces the chance for the potential victims to report crime to the authorities. Otherwise, scam or fraud is actually a much more serious criminal offense than email spam itself and usually warrants more attention from law enforcement.

To date, there is no reliable estimate on how many people actually fall victim to these scam emails every year and the cost of such scam remains unknown, but the number is likely to be in billions including all direct and indirect costs plus the resources spent on preventing such scam (Anderson et al., 2013; Whitty, 2013; LexisNexis, 2017). Certainly scam needs not always rely on email spam to carry out and the motive may not always be financial (Whitty, 2013), but in this chapter the focus is on how email spam may lead to scam and fraud. The link between email spam and scam is important as the content of scam emails may serve as evidence and the header information in each email, despite the likelihood of spoofing, could provide traces leading to the criminal's location (Yu, 2011).

Illegal Transactions

Although scam or fraud is a common theme in email spam, most spam emails are being used as advertisements (Yu, 2011). Generally, spam is a cheap way to promote a business on the Internet. The main benefit of using email spam for advertising lies in its ability to reach a very large population with little time and technical difficulty. As mentioned above, the FTC does not exactly ban sending commercial emails as long as the regulations are met. Spammers do not particularly care about those regulations however (Yu, 2011; Yu, 2014), mainly because of the small perceived likelihood of them being caught and punished in spite of the CAN-SPAM Act. Spammers are more concerned about how to make sure the email arrives in the recipient's inbox rather than the spam folder. Their biggest obstacle is the spam filters, not legal deterrence (Yu, 2011). Although most spam emails will not pass the spam filter and even if they do very few recipients would pay much attention to what is being advertised in the email, unsolicited commercial emails are still rampant on the Internet. Since the cost and risk are both low, many online merchants who cannot or would not afford traditional advertising still view email spam as one viable way to draw at least some attention to their business. These are the merchants who run an otherwise legitimate business and they just need a way to reach potential consumers. In contrast, for the merchants who are running an illegitimate business, email spam for advertising is even more fitting to their criminal activity.

In theory everything can be advertised in email spam, but the most commonly seen products are drugs and pornography (Yu, 2011; Yu, 2014). The drugs being advertised are usually prescription drugs coming from unknown sources. There is little guarantee they are authentic drugs, which makes the potential harm of this type of email spam much greater than simply an annoying email. It can pose a threat to public health. It is a well-known fact that drug abuse is a serious issue around the world, so conceivably there must be a market for this type of business. Aside from prescription drugs, illegal drugs can also be distributed this way. Many of these illegal transactions take place on the Dark Web (Maddox et al., 2016), but there is still a need to advertise the products first before people know where to look. This is when email spam becomes helpful. Normally, the instructions regarding how to complete transaction are not obvious in the spam email. Usually there is a link in the email leading potential clients to more instructions or contact information, but the link is usually time-sensitive to avoid being traceable. Unlike those merchants running legitimate businesses, online drug sellers do not usually make an effort to beat the spam filter (Yu, 2011). They are fine with their emails being flagged as spam, because their clients usually would actively look for these emails to initiate transaction. Besides, similar to scam, hiding drug-selling emails in the spam offers protection due to the low-key status of email spam.

Other than drugs, pornography is also a commodity regularly appearing in email spam. Sex-related crimes will be discussed in detail in the next section. A less common or less obvious crime hidden in email spam is e-fencing. Fencing is a century-old practice closely related to property crime. After crimi-

nals steal property, they usually need an outlet to sell the stolen property in a clandestine manner so that the police cannot trace the property back to the offender. This outlet has to be reliable and resourceful. The person providing such an outlet is called a fence and the practice of selling stolen property is called fencing. With the help of technology, today's fencing can be efficiently done electronically (Carver, 2014; Yu, 2015b). E-fencing reaches a larger pool of potential customers and allows the transaction to transcend geographical limits. In addition, the cyberspace always provides a certain degree of secrecy that is very appealing to criminals. Not unlike merchants who need advertising to promote business, e-fencing needs to promote their products to potential buyers as well. As such, email spam is a good option for e-fencing. Although technically there is no practical reason to stop the fence from just listing the products on Amazon or eBay or craigslist, some stolen property is unsuitable to be sold so publicly. In this case, the use of email spam is not aimed at reaching a large group of audience. Rather, it is using spam as a disguise. The advertisement might appear to be promoting some common items, but the true intention is to inform insiders of the availability of certain commodities. In fact, this tactic could be used by drug sellers as well. When the supply is limited, there is no need to advertise it to too many people but it is still imperative to notify insiders of the availability. In a way, it is a method of masquerading incriminating communication as email spam. How email spam facilitates covert communication will be discussed further in a later section.

In sum, email spam can be a gateway to a criminal world where illegal transactions are taking place. Since this criminal world could position itself on the Dark Web and become relatively hard to find, it still needs to attract more clients from regular Internet users and email spam is one way of advertising it without drawing too much unwanted attention.

Sex Crime

As mentioned, for the most part email spam is being used for advertising. Sex is one of the commodities that could be the center of such advertising. In fact, sex is one of the most prominent themes in email spam (Yu, 2011; Yu, 2014). Pornography is rarely being advertised openly in conventional media but it is easy to find on the Internet nonetheless. Many pornographic websites, such as Pornhub frequently rank high in the most visited websites list (Alexa, 2018). However, not all pornographic videos or photos are free to be shared online. Some are made for profit and being shared or sold without the copyright holder's permission, which constitutes copyright infringement. As such, even if the content of pornography is not illegal, the sharing and selling of it could be illegal. Similar to what was discussed in the previous section, illegal transactions of pornography oftentimes rely on email spam for advertising. Other than pornography, sex-enhancement drugs and toys are also popular commodities frequently advertised in email spam. Although mostly these are simply some people trying to sell their products and the use of email spam entails nothing more than advertising, there are some scammers who would incorporate sex into their scam schemes. It could be a scam in which the buyer pays and does not receive the product, or they might receive counterfeits. When it is sex-related, the victims are less likely to report it to the police because most of them find it embarrassing to disclose what they were trying to buy and this is what the scammers are counting on. How many people would want to tell the police they tried to buy Viagra online and got scammed, for instance? For scammers, sex is so enticing and unspeakable that it is a perfect ruse to be deployed.

However, scammers do not merely rely on shopping scam when it comes to sex. An emerging trend is online romance scam. In this crime, criminals pretend to initiate an intimate relationship through an online avenue, and after gaining trust the objective is usually to defraud the victim of money (Whitty &

Figure 2.



Buchanan, 2012). This form of scam mostly occurs on online dating sites or some classified advertisements being used by many people to seek romance. These dating sites are ideal for a hunting ground because when the victims already possess a mindset to actively look for intimate relationships, it is fairly easy to manipulate them into trusting a scammer wearing a “true love” disguise. However, in addition to targeting romance seekers, some scammers also resort to email spam to widen their net. Figure 2 is an example of spam email of this type. The content of the email links to another website that features many female photos with seductive messages. It could be a scam or a simple advertisement, but its sexual connotation is no question.

Most sex-related spam emails are promoting something that does not necessarily need to hide on the Dark Web. Hiding in spam could suffice in most cases. Nevertheless, some sex-related commodities are much more suitable to be kept on the Dark Web as hiding in email spam is not dark enough, such as child pornography and human trafficking for sex. Porn exchange is fairly common on the Internet, including the Dark Web (Chertoff & Simon, 2015). On the Dark Web, the main appeal is that anonymity is usually easier to achieve. Many Dark Web social networks have emerged for like-minded people to become associated more conveniently without the state regulation, and pedophiles certainly are utilizing them (Bradbury, 2014; Gehl, 2016). While some of these criminal networks are intentionally being kept in small circles, others are definitely trying to expand their clientele and attract more business. In this regard, email spam once again is sometimes seen as a suitable way of advertising. A close examination of this type of spam emails would reveal that some advertising emails do not link to a website accessible from a regular web browser. Instead, these advertisements contain only instructions for accessing the Dark Web (Yu, 2015a). These instructions may be hard to discern for those who are not particularly familiar with the Dark Web, and they might even be encrypted. It is not uncommon to see coded messages in email spam (Yu, 2015a), but most people tend to dismiss them as gibberish as one would expect to see in junk emails. How email spam can be used to convey covert messages is discussed in more detail in the following section.

Covert Communication

Email is essentially a tool for communication. It is convenient because of its extremely low cost and its prompt delivery for the most part. While in modern days most people probably prefer to send text messages through a cell phone, email still holds its place in electronic communication as it allows for longer and more organized messages to be sent. With HTML, the content of an email can be a lot more

enriched and artistic if needed (Yu, 2011). However, in the criminal world, the primary concern is usually about being untraceable whereas being untraceable oftentimes implies inconvenience. In this regard, email spam provides an option for criminals to communicate with a lower risk of being detected and at the same time still enjoy the benefits of email, such as low cost and promptness. It is important to note that criminals certainly may use a variety of methods to facilitate covert communications and it is by no means being suggested that email spam is the primary method or the best method. Nonetheless, it is a viable option particularly because of the lack of attention email spam is receiving.

Mainly, there are five general methods that can be applied to email spam in terms of covert communication. First, the message can be inserted in an advertisement and disguise as spam. Without a close look, most people would not notice the message. Even if they notice, they probably will not know what that message is referring to. Usually the intended recipient is the only person who knows the context enough to make sense of the message. For instance, the message may contain information about time and location without clarifying what this information is for, but the intended recipient should know (Yu, 2015a). Second, encryption may be used. More sophisticated criminals, such as terrorists, would want to further disguise their messages by means of encryption (Yu, 2015a). Anyone can easily create a coded message but the real challenge is whether the recipient can decrypt it. For example, `upnpsspx` is an encrypted word for “tomorrow”. The encryption is fairly simple as it shifts each letter to the next letter in the alphabet. However, if the recipient does not know that, then `upnpsspx` is a meaningless word, and thus communication will not be successful. In this case, again the criminals on both ends of communication should possess some prior knowledge about the context so as to communicate effectively with encrypted messages. When encrypted messages appear in a normal email, investigators would naturally want to decipher them and therefore the risk is higher. In contrast, when encrypted messages appear in spam emails, most people would not think too much about it, because random text has been commonly seen in spam emails since inserting random text is one of the popular ways in the effort to deceive spam filters (Yu, 2011). The purpose is to mislead the spam filter to believe the message is unique since each one has a different text string inserted, which may reduce the chance of being flagged as spam. Encrypted messages may look like such random text and therefore be overlooked.

Third, a message may not be revealed in the email itself as email serves as merely a link to a different place (Yu, 2015a). As mentioned before, many spam emails contain only a link to another website. Criminals could use these links to guide the recipient to where the message is hidden. The message could be hidden on a blog in one of the articles or in the fine prints on some credit card application website, for instance (Yu, 2011). Lately, some voice message services allow people to leave a voice recording and the intended recipient can access the voice message through a link in the email. This way, there will be no phone record but the voice communication can still be accomplished. In addition, it can be hard to trace or prove who is leaving such messages. Disguising this type of email as spam offers deniability because the recipient can deny being the intended recipient, since spam supposedly is sent to multiple random people at once.

Fourth, steganography is a technique that is widely used to hide an electronic file inside another electronic file and therefore the hidden file becomes hard to be detected. For instance, a pedophile may hide child pornography inside an innocent looking vacation photo. Without a further analysis, it is very easy for such incriminating evidence to be overlooked. With steganography is incorporated into email spam, it provides double disguise for covert communication (Yu, 2015a). It is not uncommon for spammers to use images as the content of their email. The image usually looks like regular advertisement. Inside the image, however, something more sinister could be hidden. It could be a text message, a picture, a document, or even a recording. Most people, including criminal investigators would tend to see only what

the image looks like without suspecting other electronic files could be hidden inside. This is inevitable considering the volume of electronic files one may discover in any given device or any online account, such as Instagram. It is simply infeasible to take a close look at every file. By far, there is no forensic software that can offer a quick scan through all electronic photos uncovered in a device and reliably flag possible use of steganography. Hence, steganography can be a very effective tool for communication among criminals to be undetected. On the other hand, if the recipient does not realize there is a hidden file or is unable to extract it, then steganography will actually defeat the purpose of communication.

Fifth, forged header information in a spam email could contain the real message rather than in the content (Yu, 2015a). It is a known fact that many spammers consistently use false information in the header, such as a fake sender's email address (Yu, 2011). It is a blatant violation of the regulations stipulated in the CAN-SPAM Act, but as mentioned, spammers are not usually too concerned about the Act. Using a fake name or email address normally is an attempt to conceal the true sender's information and to make the email look believable. For example, when the purpose is scam, by using forged header information scammers try to let the recipient believe the email comes from a legitimate source, such as your bank or school. Since it is a common tactic employed by spammers, no one would find it suspicious when criminals are actually using the header to convey the true message instead of the content. The content may look like regular spam advertising or it could be empty. It has been found that criminals could use fake header information to provide instructions on how to access the products on the Dark Web (Yu, 2015a).

In sum, while spam email has rarely been taken seriously, its low-profile status offers ideal disguise for criminals who do not want their communication to be detected. Making personal communication look like email spam could avoid attention since everyone using email nowadays would typically receive several spam emails on a daily basis and thus become insensitive to it. Even if the message is being suspected, spam offers deniability because spam usually targets a large group of random recipients. It is important to note that sometimes the email is merely designed to look like a spam email but the message is still only sent to the intended recipients, whereas sometimes criminals use real spam to send a message, in which case many random people could receive the same message but they will not know the significance of it. Either way, when the communication is covert in nature, the intended recipients need to possess some prior knowledge so as to know what to expect and how to use the information they receive. Otherwise, cover communication by means of email spam might deceive not only the authorities but also criminals themselves.

Malware

A recent trend has emerged as more and more malware is being disseminated through email spam. This type of spam is usually referred to as malspam. According to Multi-State Information Sharing & Analysis Center (MS-ISAC), malspam has become the number one method by which malware is being sent to unwitting people around the world (MS-ISAC, 2018). There are many types of malware. One common purpose is to function in the background of a computer system without the user's knowledge, and thereby provide remote access for the criminals (e.g. Trojan). The malware may be logging key strokes so that criminals would know what you type in for passwords, or malware may be stealing data from the infected computer and transmitting such data to the hackers. Some malware, also known as ransomware, could freeze a computer and thus deny the rightful user access until the user pays a ransom, usually in the form of cryptocurrency, such as Bitcoin (Patil & Patil, 2016; Chen et al., 2017). Ransomware may simply lock or encrypt the data but some more malicious variants could wipe the hard drive clean even when the ransom has been paid. Malware also is commonly used to create a botnet that can be used for criminal

purposes, such as launching denial of service attacks or secretly using other people's computers to mine cryptocurrency. Since almost no one would voluntarily download or install malware onto their computers, a clandestine way of spreading it becomes imperative for criminals. As such, email spam provides a way. Similar to using email spam to send advertisements or scam emails, malware can be hidden in a spam email with click bait. Once the recipient clicks on the link or downloads the attachment, malware could be successfully landed in the computer system. Recently, one frequently used ruse in malspam is fake mail delivery notification. In this type of spam, the email usually appears to come from UPS or FedEx notifying you that you have a package waiting for you and you should click on an embedded link to see more information. Typically the link would trigger downloading of malware that the user might not notice (Tellenbach et al., 2016; Matwyshyn, 2006). The distribution of malware used to heavily rely on pop-up windows that are associated with many underground websites that promotes pornography or online gambling. Usually users need to click on quite a few of those advertising windows before they can finally see what they came there to see. While users think they are simply closing those pop-ups, through clicking they probably have unknowingly introduced some malware onto their computers. This method has been largely ineffective now as more people are using ad-blockers to avoid these pop-up windows from showing. As a result, malspam became a new favorite method.

The personal data collected through malware could be sold in the black market, especially when such data are stolen from government agencies. Government agencies and big companies are among the most popular targets when it comes to malware (MS-ISAC, 2018). However, criminals certainly do not mind collecting some sensitive information from individual users as well. Many criminals attempt to plant malware even though they may not possess any advanced knowledge about computer networking because there are tools readily usable to disseminate malware. They may be found on the Dark Web and might even be attainable by a simple Google search. Once again, email spam provides such operations with some protection by means of its low-profile crime status and low cost.

SOLUTIONS AND RECOMMENDATIONS

Given the close links between email spam and other crimes, there is a need to develop better techniques or programs for further analyzing spam emails and tracing their origin. The volume of spam emails that are being sent on a daily basis is amenable to the generation of big data, when they are systematically collected. Analysis on such data can potentially uncover more about email spam's involvement in the criminal activities taking place on the Dark Web or otherwise. It is unrealistic to assume the Dark Web is somehow completely separated from the rest of the Internet. Criminals do not always stay in the dark. Email spam has been used as the gateway to the Dark Web and it has served as one advertising method for Dark Web marketing, such as drugs, guns, child pornography, and sex slaves (Yu, 2015a; Yu, 2015b). Email spam can also be used by terrorists to hide communication (Yu, 2015a). Since spam emails may contain multiple languages and various coding schemes, a more consolidated effort as opposed to individual projects is warranted to perform comprehensive analysis on spam emails. Before this can happen, both practitioners and academics need to recognize the full potential of email spam in terms of its criminal involvement, which is much more than the scope of the CAN-SPAM Act. For email users, to reduce the risk of being victimized by the schemes hidden in email spam, caution is much needed. Users should manually report spam and be careful before clicking on a link or downloading a file from email. Users may also report scam, malware, or other email crimes to the FBI's Internet Crime Complaint Center (IC3). However, it is unlikely for the FBI to launch an investigation for every complaint they receive.

FUTURE RESEARCH DIRECTIONS

Currently, most research about email spam is only devoted to training spam filters to accurately identify or block spam. More attention needs to be paid to the content and the context of email spam. First, big data need to be generated and the data need to include a variety of sources so as to capture the full scope of spam. For example, most Americans probably never received spam emails written in Chinese or German, because the user's Internet habit will determine what kinds of spam they are most likely to receive. Omission is likely to happen if spam is collected from homogenous sources only. Second, machine learning (e.g. text analytics) can be employed to train computers how to classify spam emails based on the content and how to identify possible covert communication, such as the existence of coded messages or steganography. Third, after covert communication is detected, further analysis needs to be developed to decipher the message. Research in this regard is inevitably interdisciplinary in nature. It requires knowledge from criminology to understand criminal operations and criminal mindset. It needs expertise in computer networking to understand the Web and email systems. It also requires linguistic knowledge to analyze the content, and when foreign languages are involved some cultural understanding is crucial. Cryptography can be relevant as well in dealing with encryption. In sum, research on email spam is not new but research on in-depth spam analysis remains uncharted territory. It has merit to look further into the connection between email spam and other crimes and it calls for interdisciplinary efforts.

CONCLUSION

In this chapter the objective is to illustrate the potential connection between email spam and other crimes, such as illegal pornography, illegal drug selling, scam, malware, human trafficking, and so on. Regardless of what type of crime is being associated with email spam, the appeal offered by email spam is mainly related to the fact that very few people are paying attention to the context of spam emails as most attention is on how to block spam. Although most spam emails are indeed being blocked (Yu, 2014), spammers' endeavor continues nonetheless, which suggests spam is still serving a purpose to some extent. Researchers should not be content by keeping spam in the spam folder. Ignoring the information contained in these so-called junk emails is counterproductive in terms of intelligence-led law enforcement because intelligence can be rich in these spam emails if carefully analyzed. Such intelligence may lead to more understanding on the operations of criminal organizations and the social dynamics of the Dark Web.

REFERENCES

- Alexa. (2018). *The top 500 sites on the web*. Retrieved Oct 2, 2018 from <https://www.alexa.com/topsites>
- Anderson, R. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy*. Berlin: Springer. doi:10.1007/978-3-642-39498-0_12
- Bradbury, D. (2014). Unveiling the dark web. *Network Security*, 2014(4), 14–17. doi:10.1016/S1353-4858(14)70042-X
- Carver, C. (2014). *E-fencing detection: mining online classified ad websites for stolen property* (Doctoral dissertation).

Chen, Y. C., Li, Y. J., Tseng, A., & Lin, T. (2017, October). Deep learning for malicious flow detection. In *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on* (pp. 1-7). IEEE. 10.1109/PIMRC.2017.8292316

Chertoff, M., & Simon, T. (2015). *The impact of the Dark Web on Internet governance and cyber security*. Retrieve Oct 2, 2018 from https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

Federal Trade Commission. (2009). *The Can-SPAM Act: A Compliance Guide for Business*. Retrieved September 25, 2018 from <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>

Ford, R. A. (2005). Preemption of state spam laws by the federal CAN-SPAM Act. *The University of Chicago Review*, 72(1), 355–384.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, 18(7), 1219-1235.

Lexisnexis. (2017). *The 2017 LexisNexis true cost of fraud study*. Retrieved Sept 30, 2018 from <https://risk.lexisnexis.com/insights-resources/research/2017-tcof>

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital ‘demimonde’. *Information Communication and Society*, 19(1), 111–126. doi:10.1080/1369118X.2015.1093531

Matwyshyn, A. M. (2006). Penetrating the zombie collective: Spam as an international security issue. *SCRIPTed*, 3, 370–388. doi:10.2966crip.030406.370

McAfee. (2009). *The carbon footprint of email spam report*. Retrieved Sept 25, 2018 from <http://resources.mcafee.com/content/NACarbonFootprintSpam>

MS-ISAC. (2018). *MS-ISAC cyber crime technical desk reference*. Retrieved Oct 17, 2018 from <https://www.cisecurity.org/white-papers/ms-isac-cyber-crime-technical-desk-reference/>

Patil, D. R., & Patil, J. B. (2016). Malicious web pages detection using static analysis of URLs. *International Journal of Information Security and Cybercrime*, 5(2), 31–50. doi:10.19107/IJISC.2016.02.06

Rabinovitch, E. (2007). Staying protected from “social engineering”. *Communications Magazine, IEEE*, 45(9), 20–21. doi:10.1109/MCOM.2007.4342845

Rogers, K. M. (2006). Viagra, viruses and virgins: A pan-Atlantic comparative analysis on the vanquishing of spam. *Computer Law & Security Report*, 22(3), 228–240. doi:10.1016/j.clsr.2006.01.006

Tellenbach, B., Paganoni, S., & Rennhard, M. (2016). Detecting obfuscated JavaScripts from known and unknown obfuscators using machine learning. *International Journal on Advances in Security*, 9(3/4), 196–206.

Weinstein, L. (2003). Spam wars. *Communications of the ACM*, 46(8), 136. doi:10.1145/859670.859703

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, 53(4), 665–684. doi:10.1093/bjc/azt009

- Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 181–183. doi:10.1089/cyber.2011.0352 PMID:22304401
- Yeagain, J. W., Settoon, R. P., & McKay, S. E. (2004). Can-Spam Act of 2003: How to spam legally. *Journal of Strategic E-Commerce*, 2(1), 15–30.
- Yu, S. (2011). Email spam and the CAN-SPAM Act. *International Journal of Cyber Criminology*, 5(1), 715–735.
- Yu, S. (2014). Sex in Spam. *International Journal of Criminal Justice Sciences*, 9(1), 35–45.
- Yu, S. (2015a). Covert communication by means of email spam: A challenge to digital investigation. *Digital Investigation*, 13, 72–79. doi:10.1016/j.diin.2015.04.003
- Yu, S. (2015b). Human trafficking and the Internet. In M. Palmiotto (Ed.), *Combating human trafficking: A multi-disciplinary approach* (pp. 61–74). CRC Press.

ADDITIONAL READING

- Brunton, F. (2013). *Spam: A shadow history of the Internet*. MIT Press. doi:10.7551/mitpress/9384.001.0001
- Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital ‘demimonde’. *Information Communication and Society*, 19(1), 111–126. doi:10.1080/1369118X.2015.1093531
- MS-ISAC. (2018). MS-ISAC cyber crime technical desk reference. Retrieved Oct 17, 2018 from <https://www.cisecurity.org/white-papers/ms-isac-cyber-crime-technical-desk-reference/>
- Ormsby, E. (2018). *Darkest web: Drugs, death, and destroyed lives*. Allen & Unwin.
- Yu, S. (2011). Email spam and the CAN-SPAM Act. *International Journal of Cyber Criminology*, 5(1), 715–735.
- Yu, S. (2014). Sex in Spam. *International Journal of Criminal Justice Sciences*, 9(1), 35–45.
- Yu, S. (2015a). Covert communication by means of email spam: A challenge to digital investigation. *Digital Investigation*, 13, 72–79. doi:10.1016/j.diin.2015.04.003
- Yu, S. (2015b). Human trafficking and the Internet. In M. Palmiotto (Ed.), *Combating human trafficking: A multi-disciplinary approach* (pp. 61–74). CRC Press.

KEY TERMS AND DEFINITIONS

4

Covert Communication: Communication through methods that are designed to make such communication undetectable or unsuspecting.

Dark Web: Refers to websites that exist in an encrypted network that cannot be found by regular search engines and cannot be visited through regular browsers.

E-Fencing: Selling stolen property on electronic platforms to make it look like normal electronic commerce.

Email Spam: Unsolicited emails that are usually sent in bulk to nonspecific recipients.

Malspam: Spam emails that carry and deliver malware.

Malware: Malicious software that is designed to compromise a computer, server, or a computer network so as to gain unauthorized access or to cause damage.

Scam: A dishonest scheme used to deceive and manipulate a person into voluntarily providing valuable assets or information.

Steganography: A technique that aims to hide information or files inside an electronic file so that no one suspects such files or information is being delivered.

Classification of Spamming Attacks to Blogging Websites and Their Security Techniques

Rizwan Ur Rahman

Maulana Azad National Institute of Technology, Bhopal, India

Rishu Verma

Jaypee University of Information Technology, India

Himani Bansal

Jaypee University, Solan, India

Deepak Singh Tomar

Maulana Azad National Institute of Technology, Bhopal, India

INTRODUCTION

With the explosive expansion of information on the World Wide Web, search engines are becoming more and more significant in day to day lives of humans. In China only, there are more than one twenty million Internet users, among which just about eighty percent use search engines regularly and eighty eight percent using search engines as a key means to acquire newly appeared information (Liu et al., 2008).

Even though a search engine generally gives huge number of results for certain query, the majority of the search engine users simply view the first few web pages in result lists. Consequently, the ranking position has become a most important concern of internet service providers.

Spamming is the method of intentionally manipulating HTML pages to achieve high ranking of search engines. Spamming is exploited to deceive search engines indexing program and to gain ranking position.

The spammers exploit vulnerabilities in web application especially Blogging sites. Security issues in Blogging Websites are still exploratory and in spite of an increase in Blogging Websites research and development, lots of security challenges remain unanswered. Spamming are the most malicious threats to the web application, especially Blogging Websites (Rahman et al., 2008).

The main objective of this chapter is to examine to what level spammers could be threat to Blogging Websites. In first section the terms related to spamming are defined, and a sufficient overview of spamming will be presented in order to give the reader with an understanding of the background for the remaining Sections.

The subsequent section will present the indications and signs of spamming attacks. This section will provide the information of different categories of spam such as Content Spamming and Form Spam. A section devoted to Security Techniques including detective and preventive techniques will be presented.

The first section introduces the overview of web spamming including Content Spamming and Link Spamming, Click Spam and Form Spam. Further, this section elaborates the attacks form spamming on blogging Sites.

DOI: 10.4018/978-1-5225-9715-5.ch058

The next section presents the vulnerabilities in blogging sites their types and vulnerability scanners.

The last section presents the taxonomy of detection and prevention methods such as various forms of CAPTCHA, and Honeypot. It also explores the Data mining techniques including Support Vector Machine. At last conclusion of the chapter is presented.

TYPES OF WEB SPAMMING

Content Spamming

Content Spamming is the first and most widespread type of web spam because it exploits search engines based information retrieval models. These models are build from page contents which further ranks the pages on the bases of the page rank algorithms. As the result the spammers analyse the weakness of these models being implemented and exploit them. The different types of content spamming are Title spamming, Body spamming, Meta tag spamming, Anchor Text spamming, URL spamming (Henzinger, 2007).

As the title field is very important in the information retrieval, spammers try to overfill it in order to increase the page rank and this type of spamming where one overfills the title is called title spamming. In body spamming the body of the page is modified and injected with certain content or queries that are frequently searched. The meta-tags play a special role in document description as when we use search algorithm n search engines the results are fetched on the bases of the meta-tags on the webpage. So placing the spam in this content will be the most efficient way to spam the document (called meta-tag spamming). Anchors tag are the tags used to include links on the website so in anchor spamming the spammers create the links with the desired anchor text to get the right term for the target page. In URL spamming the content to be searched is itself injected to the URL.

Link Spamming

There are two main categories of link spamming namely

1. Outgoing Link spamming, in this the spammers have direct access to the page and can therefore add any content to the web page. They can easily copy the entire web catalogue.
2. Incoming link spamming, where the spammers try to raise the Page Rank and boost the number of incoming links to the page (Gyongyi et al., 2008).

Cloaking and Redirection

Cloaking is a way to provide different versions of a page to the user/crawlers based on the information contained in the request made or query being searched. The other way is to redirect users to the malicious pages by executing JavaScript. The JavaScript redirection spam is the most widespread and is the one of the most difficult detection spam by the crawlers.

Click Spam

In this type of spamming, attacker executes clicks for end users who have not made them.

Form Spam

Form Spam is one of the methods of submitting web forms with unwanted information. Unwanted information may be advertisements, link to offer pages, phishing URLs and abusive tests. Once the form is filled, it is usually sent to a group mail within the company and then the links are clicked by many, by which the spammer is able to generate the traffic, ad revenue or redirect them to phishing sites to collect the personal information.

The reasons behind these form spam are:

1. Probing for vulnerabilities: The web spammers hope to hijack the websites mail server through the web form and use it to relay their spam. This is all done to exploit the poorly written web scripts (called spam injection).
2. The spammer may want to get the links to some of their spam sites published on the web site being spammed.

But now a days the commercial logic behind web spam are that the modern search engines such as Google, Yahoo, Bing etc. rely heavily on inbound links to rank a web page in their index (that is, the websites with many keywords or the related content or with links on it are ranked the top websites and ranked the top positions on these search engines, and are visited most frequently hence earning the maximum revenue). Also, many websites allow the visitors to publish content on their web pages through completion of web form, example: Comment posted on blogs, “Guest Book” pages on the websites. So in order to earn more revenue from the websites or generating more traffic on the websites servers the spammers create “Bots” (also known as automated web crawlers) to seek out and find pages with forms. After finding such types of pages the bots fills out the form and submits the form, typically with the content that contains lots of links to spammy websites and other irrelevant content. Also, there are many human spammers that manually target websites and abuse their web forms. These spammers are difficult to block as they are able to cross CAPTCHAs and other security measures, but somehow they may not be able to spam a form when it comes to spam count because the frequency with which the bot will fill the forms is much less than the human frequency (Gao et al., 2012).

There are various impacts of form spam for instance, consider an example of Community Forums, which engage thousands of users daily. In such a case the automated form spam comments on the forums as the result the content is seen by number of users, should rather say a number of genuine users because there may be many more human spam users as well. These comments come in between their conversations and the users click on these links as the result this hijacks the entire thread with unsolicited messages. This may affect the website’s reputation as the user experience will spoil resulting in less users on the website and hence less return on investment. So form spam is a huge challenge for classified websites, forums and other job or property portals where lots of users visit on daily bases. So, the target websites are mainly the websites which have lead collection form or contact forms that spammers take advantage of. Sometimes, competitors target websites to create fake leads so that sales teams waste time and energy in pursuing these leads which impacts listing agents (in terms of return on investment) and lose confidence on the website as a result of the spam leads and may choose to opt out.

So, from above impacts we can conclude that the form spam do have a significant impact on the websites and the web users so we need to prevent such spam. No doubt with the advancement in the technologies the spamming has increased and the old methods to recover from this spam are failing. One of the reasons is during early days the websites were made from scratch and were then hosted on

the domains but now a day's everything is done online and on-click. Now a days the user just pay for the things and everything is ready in few minutes. No doubt the work efficiency has increased but spammers have found new ways to spam the content but the research is still in progress to find the methods and techniques to prevent and defence against spamming attack.

VULNERABILITIES IN BLOGGING SITES

Vulnerability Definition

Vulnerability is a cyber security related term which can be defined as a defect, imperfection, weakness, or inadequacy of a system that can leave the system open to attacks. Such imperfection or defects leaves the information security exposed to threats. Due to advancement in technology and digitization it has caused a need to prevent the data from manipulation and further attacks. Vulnerabilities make it possible for the attacker to target system to run their code on the system to exploit information (Ten et al., 2008).

TYPES OF VULNERABILITIES IN BLOGGING SITES

User Enumeration

User Enumeration is a common type of web application vulnerability. This type of vulnerability occurs where there is login page and forgot password functionality. This is done by a hostile user by use of brute force to guess or confirm the valid user.

In a login form if user enters wrong username then server returns a message depicting that the Invalid Username and in the same way if the password is incorrect server return a message depicting Password Incorrect and if both are incorrect then another message pop-up. The malicious actor is looking for such activities and responses by the server and the validity of login credentials so that the malicious actor can use brute force to crack the system (Shah & Mehtre, 2015).

Security Configuration

Security configuration includes all the aspects which uses security configuration. These configurations if misused negatively affect the software applications. Security configuration alludes to the security aspects that are taken care when the installation and building of computers and network devices are done so to reduce the vulnerabilities (Scarfone & Mell, 2010).

Remote Code Evaluation

Remote code evaluation is usually seen in web applications so to get benefit from others work and re-search. In this a remote code is injected in the file or string and its get evaluated by the programming parser. This behavior is not planned by the developer of that web application.

Invalidated Redirects and Forwards

Invalidated redirects and forwards happens when some web application agrees for unauthorized or untrusted inputs that may lead to redirect the web application to the URL that is contained in the unauthorized or not trusted input. By this URL redirection the attacker may cause problems by scamming and then stealing user's credentials. As the modified links is as similar to the original site therefore, it is easy for the attacker to make changes and blockhead the user (Rafique et al., 2015).

Inadequate Application Layer Protection

The application data present may be a weak link in your application which can be exploited and may cause issues in the security of system. If the attacker found the flaw or weakness of the application then he is capable of introducing changes in web application and may commit the crime. Some basic application vulnerability exploits are SQL injection, cross site scripting, cross site request forgery and others.

Vulnerability Scanner

Vulnerability Scanner is a kind of code or program that performs diagnostic phase of vulnerability assessment. It is used for inspection of potential threats at the points in the system to know security loop holes. It establish, explain and arrange the security holes in a system network. There are different types of vulnerability scanners one of the scanner is Nessus. This scanner uses common vulnerabilities and some exposure architecture so that easy cross-linking can be done between security tools. Nessus uses Nessus attack scripting language to establish threats and potential attacks. Vulnerability scans are therefore useful as they establish the weakness of system at the security holes and works according to that (Kals et al., 2006).

There are various types of vulnerability scanners:

WPScan

WPScan is a complimentary vulnerability scanner for non-commercial sites used by blog maintainers and security professionals. WPScan is used on platforms like Wordpress. It is a blackbox vulnerability scanner used in Wordpress. This is used by both professionals and developers. WPScan is a platform that keeps the site safe, but some problems can be solved by simply updating it (in case of plug-in and themes that are vulnerable). The WPScan feature includes directory indexing on discovered plug-in, sensitive information disclosure via exposed log files, vulnerability identification to compare the sites with known vulnerable sites, plug-in and themes enumeration to detect which plug-in are installed and activated, username discovery using username enumeration and many more (Sinha, 2018).

Sucuri

Sucuri was developed by (Daniel et al., 2010) . Sucuri is a well known authority in matters related to security of websites (especially wordpress). This technology is free for all Wordpress users. It works hand in hand with the other existing security software applications. It provides a set of security features to its users. Sucuri scanner detects blacklist warnings, security issues and malwares present in the source code. It helps the system administrator to ensure the security of the website. Its main features are receive

emails notification for secure issues, setup scans as a scheduled task, setup scans as a schedule task, detect website malware infections, view website security details and information and monitor blacklist status.

Pentest-Tools

Pentest is another tool that helps the developer to identify weakness in the web application. This is a platform to find or recognize unknown vulnerabilities in the system that may cause security breach. The pentest tool attack the system from inside in the same way the attacker can perform that from outside the system. There are different types of pentest tools one of them is Netsparker. Netsparker automatically recognize XSS, SQL injection and other vulnerabilities in the web applications. Its features are minimal configuration requires, full scalable solution and many more. Other than this there are many other pentest tools that are used for security of web application such as Zap, sqlmap, Acunetix, probe.ly, owasp, wireshark, w3af, Kali, samauri framework, aircrack, sqlninja, BeEF, dradis, rapid7, hping, superscan, scappy, Ettercap, etc.

THREATS IN BLOGGING SITES

Threat Definition

As per the Oxford Dictionary definition of cyber threat is as “the possibility of malicious attempt to damage or disrupt a computer or system”. This definition is not complete as it does not include the attempt to steal the data or access files or infiltrate data. So this definition defines the threat as a possibility but in terms of cyber security community, the threat is defined more closely to an actor or an adversary who is trying to gain access to a system and have enough potential to do any damage to it.

So in general terms completing the definition of threats in terms of computer networks and network security, threats are the potentials that may cause harm rather serious harm to the computer systems. So in formal terms threats are the potentials for the vulnerabilities to turn to the serious attacks, which are sufficient enough to cause any damage to the network and are capable enough to put the network security to risk and hence may be a cause of high business damage.

Threats can include various types of viruses, trojans, back doors so as to outright attacks from the hackers. As the majority threats involve multiple exploits so the term blended threat is more accurate when we refer to such attacks.

Types of Threats in Blogging Sites

In 2012, Roger A. Grimes a columnist enlisted these five as common security threats: Social Engineered Trojans, Advanced Persistent Threats, Phishing, Unpatched Software (such as Java, Adobe Reader, Flash), Network traveling worms.

But with the advancement in technology and the use of internet in each and every field lead to more threats and in 2016, Bob Gourley shared a video that contained comments about the security and protection technologies regarding the emerging threats to cyber security and their implications. That video talked about two major aspects that were emerging at that time first Internet of things and second Explosion of data. Today, the list of cyber threats could be seen in other way.

Injection Attacks

Injection attacks falls into the category of those attack vectors that makes the attack capable of injecting not trusted input into the source code. These injected inputs afterwards get processed by the interpreter as a query or command during the execution phase. These attacks are the most dangerous ones for web applications. These may cause data loss, data theft, denial of service and many other problems.

These injection attacks are a major concern in web security. It allows the attacker to attack the program from inside rather than from outside. SQL injection, cross site scripting these kind of attacks falls into the category of injection attacks. These are not only dangerous but are widespread in most of the legal applications. But for these attacks many software applications are present to prevent the system from damage.

SQL Injection

SQL injection is the most common type of attacking technique where the attacker injects the code into the program, query onto a system to execute distant commands. This attack may destroy your database. In this attack placement of malicious program is done between the code. The main purpose of this attack is to manipulate the database or to extract the data. This is used to attack the data-driven applications. Therefore, SQL injection may cause adverse affect on business too. By influencing an SQL Injection, in good circumstances, an intruder can use it to attack web applications. It can affect authentication and authorization mechanisms and intruder can retrieve the contents of an entire database. It can also be used to add, modify and delete records in a database. And give opportunity to the attacker to unauthorized access to sensitive data which may include information regarding customer, personally identifiable information, property information and much more sensitive information (Halfond et al., 2006).

Code Injection

Code injection is the malicious introduction of code into a system. The code injected in the application is capable of intruding database integrity. It can also create privacy, security issues. It can also change data and because of this even data correctness comes into picture. It is also done with the intention to steal data. It also can take control over the bypass access and authentication control. Code injection attacks can multitude applications that are based on user input for execution. Even the SQL injection also falls into the category of code injection. Other types of code injection are script injection, shell injection and dynamic evaluation. It is used to alter the data to give false data. Code injection attacks are not easy to find. There are many solutions that have been developed to find these for both architecture and application. Some of the examples are parameterization, input validation, addition of extra layer of protection, privilege setting for different actions, and many more (Vogt et al., 2007).

Cross Site Scripting

Cross site scripting is also an injection attack. In this type of attack the attacker adds malicious data into the content from other trusted sites. Cross-site scripting attacks takes place when an unreliable source is licensed to inject its own code into an application or web application. The malicious code is added with dynamic content sent to end browser. There are three different types of XSS stored, reflected and

DOM based XSS. Different methods are present to prevent this attack one of the methods is escaping user input, sanitizing user input, input validation (Moore & Clayton, 2007).

Phishing Attack

A Phishing attack is a security attack that tries to gain delicate, private information. Such kinds of attacks are basically done where authentication is needed such as credit card information, username and password credentials. Cyber attackers also use social engineering to influence end users for performing certain action such as clicking on a malicious link or file or some site or attackers tends to extract personal information from users data. This may cause risk to both individuals and organizations. Any kind of data is useful and sensitive; rather it is organizational data or personal data. In addition, some phishing attacks can manipulate organizations data to trick the targets into revealing sensitive information. Attackers mostly targets information regarding user's bank details, card details, company data and any sensitive information that can be important for others (Owens & Matthews, 2008).

Brute Force

Brute force attack is a best way to enter to a site or application that is being protected by password. It is a method which works in a regressive manner until the attacker gets the valid combination. Therefore brute force attack is a repetitive attack scenario. This is a computational method which is not used by common users. These methods are used by hackers and attackers to obtain valid combination. The main motive of attacker is to get illegal access and to steal valuable data. There are some precautionary measures that can be taken to prevent such attack scenario. These measures are password complexity and its length, limit login attempts, using CAPTCHA, cloudflare, two factor authentication and others (Han et al., 2002).

Backdoor Attack

A backdoor is kind of a virus that nullifies normal authentication procedural steps to start an application. This result, distant access to the resources within a system and application example file servers and databases. This makes perpetrators capable of remotely issuing system commands and upgrade malware. Backdoor installation is attained by taking lead with the help of vulnerable parts of a web application. Once installed, it becomes very difficult to detect as files tend to arrange them in a jumbled manner. These webserver backdoor are used for many malicious activities such as Data theft, Server hijacking, Advanced persistent threat (APT) assaults, launch of distributed denial of service (DDoS) attacks, Web-site defacing, Infecting website visitors, watering hole attacks.

Man in the Middle (MITM)

Man-in-the-middle attack is a kind of eavesdropping activity. Man in the middle attack is also known as a fire brigade attack. In this communication between two users is checked and changed by an uncertified client. Mostly, the attacker tends to eavesdrops and snoop by obstructing the common key message interchange and resend the message. In this process, the communication between two parties tends to be normal. This normal scenario didn't confuse the sender if the message transmitted is changed or not and if it is transmitted to the receiver or to the attacker. Therefore, the attacker controls the whole communication (Callegati et al., 2009).

SPAMMING TOOLS

XRumer

XRumer is a software made for spamming online forums and comment sections of an website. It was created by BotmasterLabs and released in the market as the program for SEO (Search Engine Optimization). This tool is able to register and write posts in the forums which is referred as forum spamming, which in turn boosts the search engine rankings. The most commonly used security techniques that most websites and blogs follow in order to detect automated spam are account registration, CAPTCHAs, e-mail verification, client detection, but this tool is capable enough to bypass all these security techniques.

This tool is smart enough as it make use of SOCKS (which is an internet protocol that helps in exchange of the network packets, using a proxy server, between the client and the server) and HTTP proxies. Hence making the it quite difficult for the sysop to block that particular source IP from which the posts are being shared. Also, this software is quite good at making and posting “Innocent-looking posts” these are generally the kind of the posts in which the questions are being asked which mentions the name of spam product. The example of such a type of comments is “Where can I get so and so product? So this tool first register itself to the forum to make the posts in the form of these innocent-looking questions and then make an another registration to post a spam link as the answer to that previously posted question and this is how the software avoids suspicions of the sysop. The side-effect of these types of posts in that that such types of posts increases the product’s rank on the search engine (such as Google, Yahoo, Bing etc.) without falling into conflict of the forums posting rules (Shin et al., 2011).

The tool is able to gather and understand AI (Artificial Intelligence) questions (questions like “What is 2+3?” “What is 4*2?” such types of questions are really common nowadays on the website security checks and are the replacement of CAPTCHA solving). Also with the advancement in technology this tool is becoming even smarter as the latest version of this tool is able to collect such security questions from the multiple sources and hence increasing its efficiency in defeating such types of questions. Here, it is also included in this tool which automatically parse the results from the search engines for the blogs and forums that can be used as the target for the XRumer application.

According to a British Technology news “The Register” (October 2008), XRumer is capable enough to defeat CAPTCHA of Gmail and Hotmail. This way after defeating this software can create accounts on these free email services and them make almost unlimited registrations on the community forums and other web sites and cause spamming. But this was only possible till these services did not change their CAPTCHA formats. So, now the users of XRumer have to use some external captcha services in order to solve the CAPTCHA on these services.

This is a great challenge for the sysops (from administrators and Web Masters) to detect these XRumer users and block so as to maintain the forums terms of services. The easiest method to deal with such types of the XRumer is to verify and approve the posts being made by the new users before it appear to the other users and visitors of the forum and if detected as spam then the XRumer will be detected and hence the IP can be blocked and kept in records. In this way if again the post in received from the same IP then it means some black-hat user of XRumer is there and this time the post will be deleted before it appears to the user.

Visual Web Ripper

Visual web ripper is a strong visual tool that is used for computerised web harvesting, web scrapping and this is also used for extraction of content from the web. This tool moves and scans all the information that is present in a website – the content structure of website as well as the search results. This is used when one needs to extract content from the websites. This tool targets the data extracts it and then send content in structured data in XML files, databases or CSV files (Haddaway, 2015).

Browser Automation Studio

Browser Automation Studio deals with creation of web applications and allows user to swiftly make applications using http client, browser, email client, and different libraries. In this Programming knowledge may be required but skills are not necessary. Major application types are spammers, uploaders, parsers, apps for the social networks, creation of posters. Browser Automation Studio supports arbitrary JavaScript execution. Projects that are compiled using BAS are independent, feasible. These do not need any other software installed on your laptops including BAS. Software operates like macro recorder: all actions that a user makes are recorded and can be played or edited afterwards (Semenov, 2013).

Integromat

It is a very strong tool that can be used manually and is the most advanced and experience based online automation platform. It is capable enough to connect applications, transfer and transform data. It works automatically and there is no user intervention needed to make this tool work. It gives direct support to the application and services with the help of HTTP/SOAP and JSON modules the user can easily connect to any of the web services. Hence allowing the user to virtually automate the entire work with just a few lines of code.

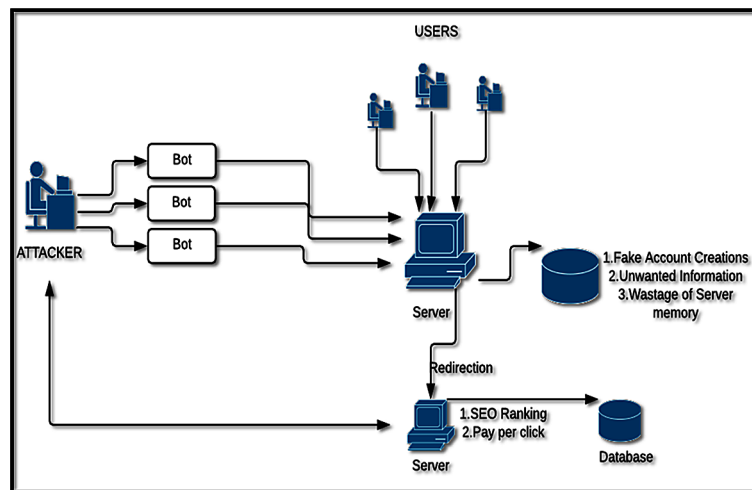
The user can also create its own application through the developer platform on this platform. So it is a quite robust tool available online and easy to use and handle. It gives cutting edge feature which makes the user capable to create its own professional integrations (Hughes et al., 2017).

Comment Anywhere

Comment anywhere is basically a program that will search the search engine for the relevant pages that suits or are similar to the search made by the user as per the user's product description, then help the user leave a comment on such web pages. It's main purpose is to save time and money which the advertisers spend in order to get the response and revenue by advertising the content and getting the positive user response.

This tool makes use of various search engines (like Google, Bing, Yahoo) so that it can cover all the relevant content as per the SEO ranking from on various search engines to make the work even more faster. This way the user can define various keyword to search on the search engines that relate to the business or the product and the tool will search on the global net for these pages and will comment automatically.

Figure 1. Block diagram for form spamming attack scenario



DEVELOPED ATTACK SCENARIO FOR FORM SPAMMING

As shown in the figure 1 is the block diagram for the attack scenario, that how the attacker attacks various vulnerable sites on the global network. The attacker first finds the vulnerabilities in the websites then with the help of various ML (machine learning algorithms) analyse the data and find out all the website on the search engine with the specific set of vulnerabilities.

This way the attacker classifies the various data as per the vulnerabilities. Then the attacker designs certain bots depending on the attack to be made on these websites in the list of vulnerabilities. Once these bots are being made then the attacker is all set and ready to fulfil its desired purpose which can be creation of fake accounts in order to post on the forum websites or to waste the opponents server memory and generate high traffic so that the server may collapse and this may further decrease the page rank and visitors to the website. Not only this, but the bots can even help is advertisements and publicity of one's own website thereby increasing the websites SEO (Search Engine Optimization) ranking and hence more revenue generation.

So the main aim of these attacks is to either collapse the opponents website, generating high revenue by increasing SEO ranking, advertising and increasing page clicks or information leak (which is against law and is information security and privacy is a great concern in today's world.)

DEFENSE TECHNIQUES AGAINST SPAMMING ATTACKS

With the advancement of technology we have various websites and portals that allows the user to develop things easily by automating everything. No doubt, this helps in saving the user time and energy as if a user wants to make a website for their business then they simple have to pay on one portal, describe the design (using few options provided) and it's all set and done. The work that use to take months is done in just few minutes and that too without hiring and expert. But, this is the reason why one needs to be more worried when it comes to security because with increasing ease of development various new threats and attacks have came into existence which were not present in earlier days. Can one image that today, globally 75.9% of the email messages are spam and reason to this is that spamming is quite profitable

and the risk involve in doing such activity is much less than the profit one can gain. From this we can conclude that somewhere we need some techniques so that the new spam can be detected and prevented in order to secure the data and reduce this global increase in spamming (Rahman, & Tomar, 2018). So here are a few commonly used and efficient detection and prevention techniques that are used for detecting and preventing spam. These techniques are based on both machine learning and non-machine learning algorithms. Various systems are introduced for automatic classifications as Bayesian classifiers, Support Vector Machine (SVM), Decision Trees, Neural Networks and sample based methods.

Detective Techniques

Link Based Learning Algorithm

It is a link learning and self-training algorithm which involves the use of classifiers and the self-learning capability of these classifiers and the topological dependency on the web graph. The classifier used is first trained with the small training dataset in link learning. The trained classifier is then used to detect and classify the unlabelled data in the data set being collected from various websites (the dataset maybe the IP addresses or the posts being shared or the registers users email). After labelling the data the spamicity value is predicted. This way in the link learning step first the unlabelled data is classified and then the link spamicity of that data is calculated (Geng et al., 2009). This way the largest and smallest samples are converted into labeled ones based upon values of link spamicity (with their predicted tables).

$$Ps(x) = \frac{p_{spam}(x)}{p_{spam}(x)} + p_{normal}(x) \quad (1)$$

$$Ls(h) = \sum_{v \in N(h)} (ps(v)) \times \text{weight}(h, v) / \sum_{v \in N(h)} \text{weight}(h, v) \quad (2)$$

where v, h are the hosts, $\text{weight}(h, v)$ is the weight of host h, v , $\text{weight}(h, v) \in \{1, n, \log(n)\}$, where n is number of hyperlinks between h and v between h and v . $N(h) \in \text{inlink}(h)$ or $\text{outlink}(h)$. $\text{inlink}(h)$ represent the link set of h , and $\text{outlink}(h)$ is the outline set of h .

$$Ls(h) = \sum_{v \in N(h)} (Ps(v) * \text{weight}(h, v)) /$$

Markov Clustering

Markov Cluster Algorithm abbreviated as MCL algorithm was given by Stijn van Dongen at the Centre for Mathematics and Computer Science in Netherlands. This algorithm is a fast and scalable unsupervised graph clustering algorithm based on the simulation of stochastic flow of graphs (Van, 1998).

As mentioned, MCL is an unsupervised graph clustering algorithm, describing this term. Unsupervised learning and clustering are closely related in pattern recognition systems. Graph clustering is the clustering of the graphs in such a way that the vertices of the graph are grouped into clusters taking into consideration the graph's edge structure. The clusters are made in such a way that there few edges

between the clusters and many edges within each cluster and the basic task of the unsupervised learning is to classify the data set into two or multiple classes based on various similarity measures over the given data set, without adopting any theoretical information regarding classification.

AdaBoost Classifier

Freund and Robert Schapiro proposed this machine learning algorithm. To improve the performance of this algorithm the meta algorithm is used in aggregation with other learning algorithms. This AdaBoost classifier (works with the concept of active learning) make use of confidence based label sampling. The classifier is trained, the training is done by variance and the scoring function is obtained, which is further used to classify the data as spam or non-spam. This means that the data one used as the input is classified as spam and non-spam and the function that is used to classify the data as spam is used generated by this training classifier. This way by using this Meta algorithm the training process is improved. The classifier is used in a series of rounds (recursively) $n=1,2,3,\dots,N$, and for each recursive call a distribution of weights $D(n)$ is updated. These weights indicate the importance of each record in the corpus for the classification.

A few more approaches are used for spam detection, these approaches mostly include K-Nearest Neighbour algorithm and pre-classified data sets which serve the purpose of training data (which helps in the learning process). The classification of the posts or messages is done with the help of KNN algorithm based on various set of features. As if one wants to filter out the spam from the mails then firstly the mails are selected from the inbox and then after analysing it, feature extraction is done. The features may include Number of replies, Number of recipients, Size of the message, Number of attachments and soon. Then with the help of KNN algorithm the data classification is done and F-measure is calculated to obtain the results (Ahmed & Abulaish, 2012).

PREVENTIVE TECHNIQUES

Form Validation

Form validation means adding certain check to the input fields in the form, to avoid the user to submit junk data through the forms. This is mainly done by the developer of the form while coding (mainly using JavaScript in HTML or any other client-side language), but nowadays the users are not making the websites from scratch so the online websites have various plug-ins for the same. Also, many websites use third party tools for form validation as Web-Form-Buddy, Parsley etc. Many common web-bots are detected by the form validation but a few very clever pass these form validations too. So, form validation is one of the great way to eliminate the significant amount of form spam.

Data Confirmation Screen

When the form is filled then a data confirmation screen is displayed which shows the copy of the data being entered for submission by the user. If the user is a web-bot, then it will not be able to confirm the data entry and in this way we can prevent from spam.

Use of CAPTCHA

This is one of the most popular way to prevent form spam. It works by generating a random text (generated using server-side languages) or more complex expression (which don't have any specific pattern so that it can be detected by any web-bot) and stored in a session. Then this text or the complex expression is drawn over an image and included in the form and user has to input that text prior to submission. If the text is not valid (which is compared on the server side) then the form is not being submitted (Rahman et al., 2012).

No doubt, this technique was designed considering the fact that it is easy for the user to detect the CAPTCHA, unlike the bots. But this was true in past, now with the advancement in technology and human minds the quick evolution of OCR programs have helped spammers to solve the CAPTCHA.

The Google's new No CAPTCHA or reCAPTCHA simply ask the user to confirm "I am not a robot" and most of the users simply click it and are able to fill the form but a few (for those the google intelligence algorithm is suspicious about) may have to pass the CAPTCHA test. Google's reCAPTCHA is a very powerful anti-spam device which is also helping the public-service to help digitize text, annotate images and build machine learning datasets and help solving hard artificial intelligence (AI) problems.

Honey-Pot

It is again a new technique to detect the spam and filter it out from the rest of the from submissions. This technique relies on the assumption that the spam or the web bots does not recognize CSS (cascading style sheet) and JavaScript. The honey pot is basically a trap in which the spam thinks that it is working in a right way but in actual it's being befooled by using a non-visible field, as the less intelligent bot which automatically fills out the fields prior to from submission will fill all the fields (including those fields which are hidden from the human eyes). As, the result one can detect that an web-bot attack has been made and the following entries are spam (Rahman & Tomar, 2018).

But again this techniques works for only the web-bots that are not able to detect the CSS or JavaScript and fails for those who are able to detect.

IP Filter

In this technique a list is created which stores all the IP addresses from which the spam has already being received, this list is regularly updated with every spam detection. Then this list is used to filter out the requests to the web from. Regular expressions are used for more advanced and flexible IP filtering.

CONCLUSION

As explained in the chapter, even though there are many advantages of web applications specially blogging sites but there are lot of practical issues related to blogging sites security needs to be answered. Similar to any web application, number of security issues confronts blogging applications. In this chapter security mechanism of (Detection methods and prevention methods) web applications from spamming attacks are reviewed, and the primary characteristics and elements of spamming are also examined. It is revealed that these attacks have a severe impact on web applications and the attacks may lead to the

serious problem for search engine optimization. Nearly all key attacks of spamming along with the possible impacts and the available countermeasures have been described.

REFERENCES

- Ahmed, F., & Abulaish, M. (2012, June). An mcl-based approach for spam profile detection in online social networks. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 602-608). IEEE. 10.1109/TrustCom.2012.83
- Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security and Privacy*, 7(1), 78–81. doi:10.1109/MSP.2009.12
- Gao, H., Chen, Y., Lee, K., Palsetia, D., & Choudhary, A. N. (2012, February). Towards Online Spam Filtering in Social Networks. *NDSS*.
- Gao, Y., Yang, M., Zhao, X., Pardo, B., Wu, Y., Pappas, T. N., & Choudhary, A. (2008, March). Image spam hunter. In *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on* (pp. 1765-1768). IEEE.
- Geng, G. G., Li, Q., & Zhang, X. (2009, April). Link based small sample learning for web spam detection. In *Proceedings of the 18th international conference on World wide web* (pp. 1185-1186). ACM. 10.1145/1526709.1526920
- Gyongyi, Z., Berkhin, P., Garcia-Molina, H., & Pedersen, J. (2006, September). Link spam detection based on mass estimation. In *Proceedings of the 32nd international conference on Very large data bases* (pp. 439-450). VLDB Endowment.
- Haddaway, N. R. (2015). The use of web-scraping software in searching for grey literature. *Grey J*, 11(3), 186–190.
- Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In *Proceedings of the IEEE International Symposium on Secure Software Engineering* (Vol. 1, pp. 13-15). IEEE.
- Han, H., Lu, X. L., Lu, J., Bo, C., & Yong, R. L. (2002). Data mining aided signature discovery in network-based intrusion detection system. *Operating Systems Review*, 36(4), 7–13. doi:10.1145/583800.583801
- Henzinger, M. (2007). Search technologies for the Internet. *Science*, 317(5837), 468–471. doi:10.1126/science.1126557 PMID:17656714
- Hughes, K., Lecky-Thompson, J., Ammon, M., & Murphy, H. (2017). *Track the impact of your publications*. Academic Press.
- Kals, S., Kirda, E., Kruegel, C., & Jovanovic, N. (2006, May). Secubat: a web vulnerability scanner. In *Proceedings of the 15th international conference on World Wide Web* (pp. 247-256). ACM. 10.1145/1135777.1135817
- Kc, G. S., Keromytis, A. D., & Prevelakis, V. (2003, October). Countering code-injection attacks with instruction-set randomization. In *Proceedings of the 10th ACM conference on Computer and communications security* (pp. 272-280). ACM.

Liu, Y., Cen, R., Zhang, M., Ma, S., & Ru, L. (2008, April). Identifying web spam with user behavior analysis. In *Proceedings of the 4th international workshop on Adversarial information retrieval on the web* (pp. 9-16). ACM. 10.1145/1451983.1451986

Moore, T., & Clayton, R. (2007, June). An Empirical Analysis of the Current State of Phishing Attack and Defence. WEIS.

Owens, J., & Matthews, J. (2008, March). A study of passwords and methods used in brute-force SSH attacks. *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*.

Rafique, S., Humayun, M., Hamid, B., Abbas, A., Akhtar, M., & Iqbal, K. (2015, June). Web application security vulnerabilities detection approaches: A systematic mapping study. In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2015 16th IEEE/ACIS International Conference on* (pp. 1-6). IEEE. 10.1109/SNPD.2015.7176244

Rahman, R. U., Sahu, D. R., & Tomar, D. S. (2017). Challenges in Securing ESB Against Web Service Attacks. In *Exploring Enterprise Service Bus in the Service-Oriented Architecture Paradigm* (pp. 74-96). IGI Global. doi:10.4018/978-1-5225-2157-0.ch006

Rahman, R. U., & Tomar, D. S. (2018). Botnet Threats to E-Commerce Web Applications and Their Detection. In *Improving E-Commerce Web Applications Through Business Intelligence Techniques* (pp. 48-81). IGI Global.

Rahman, R. U., & Tomar, D. S. (2018). Security Attacks on Wireless Networks and Their Detection Techniques. In *Emerging Wireless Communication and Network Technologies* (pp. 241–270). Singapore: Springer. doi:10.1007/978-981-13-0396-8_13

Scarfone, K., & Mell, P. (2010). *The common configuration scoring system (ccss): Metrics for software security configuration vulnerabilities*. NIST interagency report, 7502.

Semenov, A. (2013). Principles of social media monitoring and analysis software. *Jyväskylä Studies in Computing*, (168).

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, 11(1), 27–49. doi:10.1007/11416-014-0231-x

Shin, Y., Gupta, M., & Myers, S. A. (2011, March). The Nuts and Bolts of a Forum Spam Automator. LEET.

Sinha, S. (2018). Kali Linux from the Inside Out. In *Beginning Ethical Hacking with Kali Linux* (pp. 105-135). Apress. doi:10.1007/978-1-4842-3891-2_6

Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, 23(4), 1836–1846. doi:10.1109/TPWRS.2008.2002298

ur Rahman, R., Tomar, D. S., & Das, S. (2012, May). Dynamic image based captcha. In *Communication Systems and Network Technologies (CSNT), 2012 International Conference on* (pp. 90-94). IEEE.

Van Dongen, S. (1998). *A new cluster algorithm for graphs*. Centrum voor Wiskunde en Informatica.

Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007, February). Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. *NDSS*.

ADDITIONAL READING

Angelini, M., Blasilli, G., Catarci, T., Lenti, S., & Santucci, G. (2019). Vulnus: Visual Vulnerability Analysis for Network Security. *IEEE Transactions on Visualization and Computer Graphics*, 25(1), 183–192. doi:10.1109/TVCG.2018.2865028 PMID:30136974

Apte, M., Palshikar, G. K., & Baskaran, S. (2019). Frauds in Online Social Networks: A Review. In *Social Networks and Surveillance for Society* (pp. 1–18). Cham: Springer. doi:10.1007/978-3-319-78256-0_1

Goel, S., Kumar, R., Kumar, M., & Chopra, V. (2019). An efficient page ranking approach based on vector norms using sNorm (p) algorithm. *Information Processing & Management*, 56(3), 1053–1066. doi:10.1016/j.ipm.2019.02.004

Saini, M., Verma, S., & Sharan, A. (2019). Multi-view Ensemble Learning Using Rough Set Based Feature Ranking for Opinion Spam Detection. In *Advances in Computer Communication and Computational Sciences* (pp. 3–12). Singapore: Springer. doi:10.1007/978-981-13-0341-8_1

Spezzano, F., Suyehira, K., & Gundala, L. A. (2019). Detecting pages to protect in Wikipedia across multiple languages. *Social Network Analysis and Mining*, 9(1), 10. doi:10.1007/13278-019-0555-0

KEY TERMS AND DEFINITIONS

Click Spam: It is a process of executing clicks on behalf of user without the knowledge of user.

Cloaking: It is a process of providing different versions of a page to the crawlers.

Form Spam: It is a method of submitting web forms with unwanted information.

Link Spamming: The process of posting links on websites, discussion forums, blogs, and other web services that show user comments.

Spamming: It is an exploitation of messaging systems to broadcast unwanted messages.

Threat: The possibility of malicious attempt to damage or disrupt a computer or system.

Vulnerability: It is defined as a defect, imperfection, weakness, or inadequacy of a system.

Cybercrime in Online Gaming

4

Boaventura DaCosta

 <https://orcid.org/0000-0003-0692-2172>

Solers Research Group, USA

Soonhwa Seok

Korea University, South Korea

INTRODUCTION

Video games are readily available on several platforms, including computers, dedicated game consoles, handhelds, and mobile devices. While these games offer rich interactive experiences, their global connectivity is increasingly raising concerns about safety. For example, massively multiplayer online games (MMOs) have been described as breeding grounds for hackers and cybercriminals. Mobile games are also of interest in this connection, because they may expose players to vulnerabilities through unauthorized access to device features. With video games anticipated to grow in popularity and sophistication, it is vital to have a clear understanding of the most current forms of online risks associated with this form of entertainment.

Considerable information on the Internet speaks to cybercrime as it relates to online gaming. However, there does not appear to be much consensus on the extent to which cybercrime has impacted the video game industry and its gamers, to include conflicting views about specific forms of illegal activity. The belief that today's cybercriminals are using virtual currency in online game economies to launder money is one such example. This idea has been presented by some as a serious problem (e.g., Richet, 2013), with the game industry unknowingly being a pawn in online criminal activity. Conversely, others have contended that the premise makes for an interesting story, but that carrying out such an act would be impractical given the challenges involved (e.g., Messner, 2018).

This chapter extends the work of Seok and DaCosta (2019), who examined the online safety practices of video game players and the degree to which they are exposed to online threats, by offering a deeper understanding of the types of cybercrime that affect the video game industry and its players. Although considerable effort was made to capture peer-reviewed materials, the great majority of the content comes from Internet news articles, to include reports and commissioned studies on the video game industry. Finally, online criminal activity is ever changing, with video games in a constant state of technological advancement. Though it is expected that this chapter will be of value to educators, practitioners, researchers, and game developers and publishers, it should by no means be considered an all-inclusive reference, but rather a catalyst for discussion, debate, and future research.

CYBERCRIME IN ONLINE GAMING

Cybercrime is not new to the video game industry (Cook, 2016; Dickson, 2016). Nevertheless, the popularity and prolific growth in the number of online games have produced new opportunities for cybercriminals (Dickson, 2016), who have come to view these games and their players (hereafter referred to as “gamers”) as easy targets for making quick money through a multitude of techniques. Given that the size of the game industry rivals that of the movie industry in terms of gross revenue, and that hacking techniques are anticipated to grow in sophistication, it has been argued (Cook, 2016, 2017) that the potential for increasingly complex and dangerous online threats is a serious problem.

In the subsequent sections of this chapter, data breaches, compromised accounts and stolen data, the theft and sale of in-game items, and money laundering are discussed. Other forms of cybercrime facing the video game industry, such as the highly debated practices of piracy and reverse engineering, are not discussed. Although these threats are also important, this chapter focuses on the most deliberate types of cybercrime impacting the video game industry in recent years.

Data Breaches

At the time of this writing, data breaches seem to have become commonplace, to such an extent that data privacy and online security have become part of the national conversation. Take the two related incidents involving the U.S. Office of Personnel Management (OPM). The OPM reported that in 2015, the personal data of 4.2 million current and former federal government employees were compromised. The data included names, birth dates, home addresses, and Social Security Numbers (SSNs) (OPM, n.d.). Later the same year, the OPM reported that the background investigation records of current, former, and prospective federal employees and contractors had also been compromised. This included the SSNs of 21.5 million individuals (19.7 million of whom had applied for a background investigation; and 1.8 million non-applicants, primarily comprising spouses or co-habitants of the applicants) (OPM, n.d.). Compounding matters, the OPM reported that some of the stolen data also included findings from interviews conducted by background investigators as well as fingerprints (OPM, n.d.).

Even though victims of large data breaches have sometimes been offered identity-theft protection coverage for a few months, or even a few years (in the OPM breach, for example, victims were given coverage through 2026 [OPM, n.d.]), in many cases the data stolen do not expire. That is, while banks and financial institutions can issue new credit cards to mitigate unauthorized purchases, other stolen personal information, such as SSNs, continues to pay dividends to cybercriminals. Four years after the OPM breach, for instance, two people pleaded guilty to using stolen OPM data in identity theft cases (Weiner & Hawkins, 2018), showing the long-term consequences of such incidents.

Regrettably, the OPM breach is by no means the largest to date. The Equifax breach in 2017 resulted in the exposure of 143 million American consumer accounts (FTC.gov, 2017). The data included names, birth dates, addresses, SSNs, and in some instances, driver’s license numbers (FTC.gov, 2017). The credit card numbers of approximately 209,000 and dispute documents (with personal information) of 182,000 consumers were also stolen (FTC.gov, 2017). Further, in 2013 Yahoo admitted that the information of one billion account holders had been stolen (Burgess, 2016). Yahoo later acknowledge that the actual number of compromised accounts was three billion (Burgess, 2017).

While these hacking events specifically targeted government, finance, and telecommunications, such incidents are by no means isolated to a specific sector, and the video game industry is seeing its own share of large-scale occurrences. The most noteworthy is perhaps the PlayStation Network breach in 2011,

in which 77 million accounts were compromised (Paganini, 2016). The attack was so severe that Sony was forced to take the network offline for 23 days (WeLiveSecurity, 2015). Sony later acknowledged (*Daily Mail Reporter*, 2011) that personal information was stolen from each of the 77 million accounts, to include approximately 12,000 encrypted credit card details (WeLiveSecurity, 2015). Many believe that the PlayStation network hack is among the largest and costliest breaches so far. Sony publicly released that the breach resulted in the loss of US\$171 million (WeLiveSecurity, 2015). The PlayStation network breach shows that in addition to life-long consequences to consumers, there are also costs to those ultimately held responsible for safeguarding the data, to include legal implications. GameStop, for instance, reached a settlement agreement in 2018 in a class-action lawsuit for the loss of customers' personal information that occurred over a six-month period from 2016 to 2017 (McParkland, 2018).

Numerous other large breaches have also occurred within the video game industry; however, many have not received the same level of attention as those described thus far. For example, the online game publisher Gamigo was breached in 2012, causing the email addresses and passwords of over 8.2 million accounts to be stolen and publicly leaked (HaveIBeenPwned, n.d.). The same year, the MMO *Heroes of Newerth* was hacked, resulting in the theft of over 8 million accounts, which included the loss of usernames, passwords, and email addresses (HaveIBeenPwned, n.d.). In 2015, the gaming website R2Games was compromised, with 2.1 million accounts made publicly available. The stolen data included usernames, passwords, and email and IP addresses. Over the course of 2016, an additional 11 million and 9 million accounts were found to have been released, bringing the total R2Games incident to more than 22 million accounts (HaveIBeenPwned, n.d.). Finally, 2016 also saw the breach of the MMO *Evony*, in which 29.3 million unique accounts were stolen. The taken data included usernames, passwords, and email and IP addresses (HaveIBeenPwned, n.d.).

In addition to these examples of large-scale confirmed breaches, many alleged hacks cannot be verified (Hunt, 2016). For instance, the 2017 alleged breach against the Chinese gaming site TGBUS is believed to have included the theft of more than 10 million unique accounts, which included usernames, passwords, and email addresses (HaveIBeenPwned, n.d.). Compounding matters, breaches are not necessarily onetime events. In some instances, accounts are hacked over long periods of time. As mentioned, the GameStop breach took place over a six-month period (McParkland, 2018). Valve also revealed in 2015 that 77,000 Steam accounts were compromised over months (Dickson, 2016; Makuch, 2015) using malware that is readily available on black markets for as little as US\$3 (Dickson, 2016).

Compromised Accounts and Stolen Data

In some instances, those involved in the breaches are not focused on monetary gain but want to demonstrate their hacking abilities or expose system vulnerabilities. However, compromised accounts can be sold to other cybercriminals (Rashid, 2013; Trend Micro, 2015, 2016) for many reasons, to include identity theft and fraud (Trend Micro, 2015, 2016). In the case of the OPM breach, the two individuals who pleaded guilty to identity theft were most likely not involved in the original data hacking, but acquired the information from underground websites, such as those often referred to as being part of the dark web (Weiner & Hawkins, 2018). Further, accounts are not solely collected from data breaches; rather, cybercriminals are also using financial sector hacking (Cook, 2016) and social engineering techniques (Rashid, 2013), to include email and spear phishing practices, to steal login credentials (Tompkins, 2017; Trend Micro, 2015, 2016).

As reflected in the discussion on data breaches, game developers and publishers collect various pieces of information from their customers, such as email addresses and payment information (e.g., credit card numbers, PayPal). In addition, they also frequently collect personal information, such as name, birth year, mailing address, and even social media information (Trend Micro, 2015, 2016). Given that there are reports putting the average gamer's age at 33 (ESA, 2018), these account owners are at the prime age to hold and use credit.

It is the sheer amount of accumulated and composite data, as well as the value behind this information, that makes these accounts so attractive to cybercriminals (Rashid, 2013). When coupled with findings that people often use the same passwords for their email, social media, banking, and other important online resources, compromised accounts can hold far-reaching financial implications (Seok & DaCosta, 2014). To make matters worse, data found in stolen accounts may also be mined with the intent of putting lives at risk. That is, social engineering tactics could be employed to determine if account owners hold significant positions in large corporations or government, or have access to important information, such as U.S. intelligence (Rashid, 2013).

The Theft and Sale of In-Game Items

Money can also be illegally made by selling virtual goods. “Duping” is said to be one of the more popular practices of exploiting bugs to illegally duplicate in-game items or currency for later sale (Cimpanu, 2016). However, online games are also intensely played (Cimpanu, 2016; Cook, 2016) to legally amass in-game items (e.g., weapons, armor) or currency that can be exchanged for real-world money (Cook, 2016). The following DFC Intelligence (2010) study, undertaken in cooperation with Live Gamer, helps illustrate the popularity of such sales. Of the 4,816 mostly male U.S. and European gamers surveyed, in-game goods (i.e., items within the game and not the full game itself) were purchased by approximately 60% of those surveyed, with power-up items purchased by nearly 50% of the participants because they perceived the items would offer a gameplay advantage. The sale and trade of legitimately attained in-game items is not illegal (although some consider the practice as cheating, and thus frowned upon), in-game items connected to stolen accounts can be unlawfully sold (Trend Micro, 2015, 2016). In addition, virtual goods can be purchased with linked credit card information associated with stolen accounts. The illegally purchased in-game items can then be transferred to other accounts and/or subsequently sold (Trend Micro, 2015, 2016). The Steam data breach is an example of this, whereby cybercriminals targeted assets to be resold on Steam Trade (Dickson, 2016).

According to *The New York Times*, the sale of in-game items and currency is so profitable that in 2005 approximately 100,000 Chinese video game players were employed by gamers in other countries to farm popular MMOs (Barboza, 2005). Sweatshops have also reportedly emerged, forcing laborers to farm game currency under poor working conditions for long hours and little pay (Cybrary, 2016). For example, China has been accused of using labor camp inmates to mine in-game items (Moore, 2011) that are sold to gamers (John, 2016), with proceeds going back to the prisons (Vincent, 2011).

Money Laundering

Even more troubling is the earnings from these sales have been said to become part of real-world money-laundering schemes (Solon, 2013). The process has been described as working similarly to traditional forms of money laundering, in which legitimate businesses are used to “clean” illegally attained money (Messner, 2018). The car wash money laundering scheme in the AMC drama series *Breaking Bad* has

been offered as an example (see Messner, 2018). The Netflix original *Ozarks* is yet another example, in which a family, in debt to a Mexican drug lord, purchases legitimate businesses to launder drug money into clean, taxable income.

The same concept holds true in the cyber world. Thus, money acquired from criminal activity can be converted into in-game currencies, and then to other digital exchanges, such as Bitcoin (Sheridan, 2018). In the same way that multiple businesses can be used to launder cash, cybercriminals can use a digital currency exchange (DCE) to digitally transfer money several times between online currencies to make money difficult to trace. Messner (2018) offers an example of how money from a stolen PayPal account is transferred to multiple fake PayPal accounts, unknowingly created by victims in the example. A DCE is then used to transfer the money from the PayPal accounts to other accounts and digital currencies (e.g., Bitcoin). The money may be exchanged even further, to online gaming currency, such as *World of Warcraft* (WoW) gold coins or Linden dollars (the currency used in *Second Life*). Such currency, in turn, could be shared between multiple gamers and then exchanged again (by the respective individuals) to other online currencies.

Even if the fees associated with using a DCE could make it costly to perform multiple transactions, the example demonstrates how online gaming currency could be used to launder money. Nevertheless Messner (2018) points out how such actions lack practicality, especially if millions of dollars need to be laundered, because too many things could go wrong. For example, in addition to losing money in each transaction (because of the fees), there are opportunities to be cheated in the exchanges, the laundering might be detected, and a game developer might notice unusually large transactions, confiscating the currency and/or disabling accounts. This is plausible because, as discussed in Messner (2018), USD\$10,000 would represent a shocking amount of in-game currency. So, while the idea of laundering money using MMO worlds and the like is an interesting one, and might work on a small scale, Messner (2018) illustrates how pulling off such an effort on a significantly larger scale would be difficult.

Money-laundering claims have been no less supported, however. The 2013 report released by the United Nations Office on Drugs and Crime found that MMOs were among the most effective ways in which cybercriminals launder money because of the growth in online game currency systems and economies (Richet, 2013). Games supposedly used in money-laundering schemes have included *FIFA*, *Final Fantasy*, *Grand Theft Auto 5*, *Minecraft*, *Star Wars Online* (*The Old Republic* or *Battlefront* not specified), and *WoW* (Sheridan, 2018). Mobile games have also been identified, to include *Clash of Clans*, *Clash Royale*, and *Marvel Contest of Champions* (Ciaccia, 2018).

The aforementioned mobile games suggest that cybercriminals may be using microtransactions to launder money that might otherwise be detected in more traditional MMOs. As further discussed in Messner (2018), however, the practicality of doing so is also in question, because the game's developer or publisher would have to be involved. Furthermore, for such illegal activity to go undetected, the microtransactions would have to come from gamers who are geographically separated, and who are using unique devices and payment methods, because millions of microtransactions from only a handful of sources would otherwise be detected with payment providers. In addition, games would have to be popular, because unpopular titles would not attract the number of microtransactions needed to launder large amounts of money (Messner, 2018).

While the matter of money laundering in online game currency systems is still being debated, funds from these schemes are said to fuel other forms of illegal activities, such as distributed-denial-of-service (DDoS) attacks. One such example is said to be (Cybrary, 2016) the Lizard Squad attack in 2015 that took the PlayStation Network and Xbox Live offline, subsequently preventing gamers from accessing either service (Paganini, 2016). Worse is the claim that this laundering platform is used by terrorist

groups (Kish, 2017). This claim could possibly help explain reports that British and American Intelligence groups have spied on in-game communications within *WoW* and *Second Life*, founded on fears that online gaming worlds could become hotbeds for dangerous activity (Crecente, 2013). That is, these MMO worlds are believed to have been a way for terrorist or criminal networks to do more than move money, to include secretly communicate or plot attacks (Crecente, 2013).

THE ROLE OF THE VIDEO GAME INDUSTRY AND GAMERS IN CYBERCRIME

Just a few years back, the video game industry was perceived as not having fully grasped that it had become the target of cybercriminals exploiting several techniques, to include server vulnerabilities, DDoS attacks, in-game glitches to steal goods (Cimpanu, 2016), and gaming economies to fuel illicit activities. Furthermore, game developers and publishers were perceived as focusing on the hardening of code to prevent piracy and reverse engineering (Dickson, 2016). More recently, it has been suggested that game companies are aware that their game worlds are being used for fraud (Sheridan, 2018). Kabam, for instance, has warned gamers of misuse that may be occurring within *The Hobbit* (Sheridan, 2018). Blizzard closed the *Diablo* auction houses on the grounds that although they offered a convenient and secure environment for trading, they also undermined the game's core play (Atherton, 2015). Finally, Valve has taken steps to implement new security features in the past few years, such as two-factor authentication (McWhertor, 2015).

Gamers Are Partly Responsible for the Increase in Cybercrime

Despite such safety measures, accounts continue to be compromised, partly because many gamers are not believed to be taking advantage of new security features and capabilities (Makuch, 2015). That is, although cybersecurity professionals advocate the use of antivirus, antispyware, and firewall software, to include keeping these types of products up-to-date, gamers have been found to disable or remove security software altogether, because antivirus and related security apps are known to slow down computers, which, in turn, results in lost frame rates, thereby diminishing the gaming experience (Dickson, 2016).

Results of a Google Consumer Survey that polled 500 gamers helps substantiate this attitude. That is, the survey found that 52% of the surveyed gamers did not use security software on their gaming computers, with 36% actively turning this software off if it slowed down their systems (Abel, 2016). Seok and DaCosta (2019) reported similar findings while examining the online safety practices of 182 gamers, revealing that 35% were not regularly updating their antimalware (i.e., antivirus, antispam, antispyware) software. However, in a broader investigation of the online safety practices of 1,092 high school students, Seok and DaCosta (2014) found that 47% inconsistently kept their antimalware software updated or ignored the practice entirely. Overall, this shows that while the Google Consumer Survey suggests gamers are not leveraging security software to their benefit, the problem may be systemic, and not necessarily specific to those who avidly play video games.

In short, it could be argued that gamers are partly responsible for the increase in cybercrime, to include the loss of in-game goods by not only showing continued resistance to cybersecurity practices seen as gaming hindrances (Cybrary, 2016), but also purchasing and (possibly) selling what may be illegally attained in-game items and currency to fuel their competitive need for quick game advancement (Trend Micro, 2015, 2016). Yet, gamers may not realize that their behavior is problematic and their actions are illegal or could lead to criminal activity.

Despite the expectation that young people can circumnavigate today's technology-rich world, it has been contended that the Internet and respective technologies have put young people in situations where they must make decisions that they may not be developmentally ready to make (Miller, Thompson, & Franz, 2009). When viewed alongside the belief that they are one of the fastest groups of adopters of the Internet (Marcum, Ricketts, & Higgins, 2010), young people may be especially predisposed to online dangers.

A study commissioned by the National Crime Agency (2015) found that the average cybercriminal in 2015 was 17 years old, compared to their findings the prior year, showing an average age of 24. The study also revealed that young people (and their parents) do not understand what constitutes a cybercrime or the consequences of such. Overall, the data from the National Crime Agency study help support the position that gamers may view their actions as nothing more than an extension of their regular gameplay (Trend Micro, 2016), and not a criminal activity. Granted, it is difficult to conceive that stealing a virtual weapon from another gamer in an MMO could result in criminal charges. This mindset, however, has in part contributed to a lack of regulation on the matter, and added to the difficulty of enacting real-world legislation and, subsequently, real-world consequences (i.e., fines, imprisonment) of activities that take place in a virtual world (Jiang, 2011).

Game Developers and Publishers Are Assisting in the Prosecution of Gamers

Game developers and publishers are assisting the courts in prosecuting players. In Japan, for example, Nexon cooperated with the authorities in the arrests of three gamers for obstruction of business due to their alleged role in creating and selling 37 kinds of cheats for *Sudden Attack*, believed to have netted the perpetrators US\$78,621 (Ashcraft, 2014). Blizzard helped convict two gamers allegedly responsible for fencing stolen in-game items from *Diablo II*, viewed by the courts as felony-level theft (Atherton, 2015). Similarly, Epic Games reportedly took two YouTubers to federal court over their alleged involvement in the use of aimbots to hack the *Fortnite* game, selling their cheats for as much as \$300 (Good, 2018).

South Korea has also criminalized the creation, distribution, and use of online game cheats, sentencing those convicted with up to five years in prison and \$43,000 in fines (Chalk, 2016). In June 2017, the country also criminalized other forms of cheating, to include “boosting” (playing while using another person's account to increase the other person's rank), punishable by an \$18,000 fine and suspended two-year prison sentence (Carpenter, 2018).

FUTURE RESEARCH DIRECTIONS

One does not have to go far to find online sources that claim the value of the video game industry is appraised at over USD100 billion. These enormous sums have attracted unwanted attention, fueling cybercrime and a criminal industry said to be valued at USD50 billion annually (Deakin University, 2017). While it can be argued that video game developers and publishers have been plagued by criminal activity since the industry's beginnings, with early concerns centered on piracy and reverse engineering, the global connectivity of today's games raises more serious concerns, including online safety. That is, as the video game industry continues to evolve, moving away from physical media to cloud-based services, and the importance and value of in-game assets continue to grow, cyber threats are anticipated to worsen. For example, the growing number of data breaches alone shows the severity of the problem,

underscoring the importance for game developers and publishers to actively address these new forms of cybercrime head-on.

Also, worrisome, video game companies are not the only targets; cybercriminals also have their sights on gamers. While it is still unclear how much gamers contribute to cybercrime, and what roles they play, it is clear, however, that young people's interest in this form of entertainment is growing, as reflected in the number of console sales. Figures made available in March of 2018, for example, revealed that the PS4, Xbox One, and Switch had sold 75.28, 36.03, and 14.46 million units to date, respectively (D'Angelo, 2018). Furthermore, the belief that gamers may not be aware that their actions are problematic, but perceive their activities as nothing more than typical gameplay for quick advancement, illustrates the need for cybersecurity-related interventions and training to help gamers understand the threats, their causes, and the respective consequences.

CONCLUSION

At the time of this writing, there does not appear to be a consensus on the extent to which the kinds of cybercrime presented in this chapter have impacted the video game industry and its gamers. But it may be safe to say that online safety is a shared responsibility between the video game industry and the gamer community. Game developers and publishers should take the threats seriously by building better security into games, to advance not only the industry and technology, but to also protect users. At the same time, users have a responsibility for their own actions, to ensure that they are not contributing to today's online criminal activity.

ACKNOWLEDGMENT

The chapter authors would like to acknowledge Joshua Shearer, co-host of the podcast site *Just One Thing Gaming* (<https://itunes.apple.com/us/podcast/just-one-thing-gaming>), for his assistance in reviewing, editing, and offering game-related subject-matter expertise.

REFERENCES

- Abel, R. (2016, September). Study finds gamer cyber hygiene stinks. *SC Media US*. Retrieved from <https://www.scmagazine.com/study-gamers-actively-shut-off-security-software-if-it-inhibits-game-play/article/530161/>
- Ashcraft, B. (2014, June). Gamers hit with criminal charges allegedly made tons of money. *Kotaku*. Retrieved from <http://kotaku.com/gamers-hit-with-criminal-charges-apparently-made-tons-o-1596352729>
- Atherton, K. D. (2015, May). When virtual crimes get prosecuted in real life. A dungeon dive into Diablo's in-game crime spree. *Popular Science*. Retrieved from <http://www.popsoci.com/no-sanctuary-diablos-game-thieves>
- Barboza, D. (2005, December). Ogre to slay? Outsource it to Chinese. *The New York Times*. Retrieved from <http://www.nytimes.com/2005/12/09/technology/ogre-to-slay-outsource-it-to-chinese.html>

Burgess, M. (2016, December). Massive Yahoo database reportedly sold for £240,000 on the dark web. *Wired*. Retrieved from <https://www.wired.co.uk/article/yahoo-one-billion-accounts-hacked>

Burgess, M. (2017, October). That Yahoo data breach actually hit three billion accounts. *Wired*. Retrieved from <https://www.wired.co.uk/article/hacks-data-breaches-2017>

Carpenter, N. (2018, December). South Korean law to punish boosters passes in the National Assembly. *Dot Esports*. Retrieved from <https://dotesports.com/overwatch/news/lucios-winter-wonderland-skin-turns-him-into-a-futuristic-snow-fox>

Chalk, A. (2016, December). Creating hacks for online games could now earn you jail time in South Korea. *PCGamer*. Retrieved from <http://www.pcgamer.com/south-korea-makes-cheating-in-online-games-an-actual-crime/>

Ciaccia, C. (2018, July). Mobile games are being used for money laundering, report warns. *Fox News*. Retrieved from <https://www.foxnews.com/tech/mobile-games-are-being-used-for-money-laundering-report-warns>

Cimpanu, C. (2016, October). Online gaming currencies used to launder money for cyber-criminals. *Softpedia News*. Retrieved from <http://news.softpedia.com/news/online-gaming-currencies-used-to-launder-money-for-cyber-criminals-509177.shtml>

Cook, M. (2016, May). Why online video gaming will be the next industry under cyber attack. *Information Week. ITNetwork*. Retrieved from <http://www.darkreading.com/vulnerabilities---threats/why-online-video-gaming-will-be-the-next-industry-under-cyber-attack-/a/d-id/1325519>

Cook, M. (2017, January). What to expect – Video game cybersecurity in 2017. *Gamasutra*. Retrieved from http://www.gamasutra.com/blogs/MatthewCook/20170112/289076/What_To_Expect__Video_Game_Cybersecurity_In_2017.php

Crecente, B. (2013, December). NSA and CIA counterterrorism efforts included Xbox Live, Second Life, WoW spying (update). *Polygon*. Retrieved from <https://www.polygon.com/2013/12/9/5191408/nsa-and-cia-counterterrorism-efforts-included-xbox-live-second-life>

Cybrary. (2016, October). *Cybercrime and the gaming industry*. Retrieved from <https://www.cybrary.it/2016/10/cybercrime-gaming-industry/>

D'Angelo, W. (2018, March). PS4 vs Xbox One vs Switch global lifetime sales – January 2018 – sales. *VGChartz Ltd*. Retrieved from <http://www.vgchartz.com/article/272742/ps4-vs-xbox-one-vs-switch-global-lifetime-salesjanuary-2018/>

DaCosta, B., Seok, S., & Kinsell, C. (2015). Mobile games and learning. In Z. Yan (Ed.), *Encyclopedia of mobile phone behavior* (Vol. 1, pp. 46–60). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8239-9.ch004

Daily Mail Reporter. (2011, April). We've been hacked: Sony finally blames 'external intrusion' for PlayStation network outage. *Daily Mail*. Retrieved from <https://www.dailymail.co.uk/sciencetech/article-1380050/Sony-admits-Weve-hacked-PlayStation-Network-outage.html>

Deakin University. (2017, October). *Video game cyber crime is a \$50 billion industry: Deakin expert*. Retrieved from [http://www.deakin.edu.au/about-deakin/media-releases/articles/video-game-cyber-crime-is-a-\\$50-billion-industry-deakin-expert](http://www.deakin.edu.au/about-deakin/media-releases/articles/video-game-cyber-crime-is-a-$50-billion-industry-deakin-expert)

DFC Intelligence. (2010, March). *Consumers & downloadable items*. Retrieved from <http://www.dfciint.com/dossier/consumers-downloadable-items/>

Dickson, B. (2016, June). The gaming industry can become the next big target of cybercrime. *Crunch Network*. Retrieved from <https://techcrunch.com/2016/06/08/the-gaming-industry-can-become-the-next-big-target-of-cybercrime/>

ESA. (2018). 2018 sales, demographic, and usage data. Essential facts about the computer and video game industry. *Entertainment Software Association*. Retrieved from http://www.theesa.com/wp-content/uploads/2018/05/EF2018_FINAL.pdf

FTC.gov. (2017, September). The Equifax data breach: What to do. *Federal Trade Commission. Consumer Information*. Retrieved from <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>

Good, O. S. (2018, October). Epic takes big-time YouTuber to federal court over Fortnite hacks. *Polygon*. Retrieved from <https://www.polygon.com/fortnite/2018/10/17/17991422/fortnite-hacks-lawsuit-golden-modz-youtube-takedown>

HaveIBeenPwned. (n.d.). *Pwned websites. Breached websites that have been loaded into Have I Been Pwned*. Retrieve from <https://haveibeenpwned.com/PwnedWebsites/>

Hunt, T. (2016, October). *Handling Chinese data breaches in Have I Been Pwned*. Retrieved from <https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/>

Jiang, D. (2011). Security issues in massively multiplayer online games. *ACC 626 Research Paper*. Retrieved from <http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Security%20Issues%20in%20Massively%20Multiplayer%20Online%20Games%20X%20Jiang.pdf>

John, R. (2016, March). Outsourcing fun: Gold farming & the rise of digital sweatshops. *The Online Economy*. Retrieved from <https://onlineeconomy.hbs.org/submission/outsourcing-fun-gold-farming-the-rise-of-digital-sweatshops/>

Kish, S. (2017, May). Massively multiplayer games a platform for terrorism? *Intelligencer*. Retrieved from <http://phcintelligencer.com/2017/05/15/massive-multiplayer-games-a-platform-for-terrorism-2/>

Makuch, E. (2015, December). 77,000 Steam accounts hacked every month, new security measures deployed. *Gamespot*. Retrieved from <http://www.gamespot.com/articles/77000-steam-accounts-hacked-every-month-new-securi/1100-6433003/>

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using Routine Activity Theory. *Criminal Justice Review*, 35(4), 412–437. doi:10.1177/0734016809360331

McParkland, T. (2018, July). GameStop agrees to settle data breach class action. *Delaware Law Weekly*. Retrieved from <https://www.law.com/delawarelawweekly/2018/07/16/gamestop-agrees-to-settle-data-breach-class-action/?slreturn=20181012154716>

McWhertor, M. (2015, April). Valve adds two-factor login authentication to Steam mobile app. *Polygon*. Retrieved from <https://www.polygon.com/2015/4/15/8424587/steam-mobile-app-two-factor-login-steam-guard>

Messner, S. (2018, April). How microtransactions and in-game currencies can be used to launder money. *PCGamer*. Retrieved from <https://www.pcgamer.com/how-microtransactions-and-in-game-currencies-can-be-used-to-launder-money/>

Miller, N. C., Thompson, N. L., & Franz, D. P. (2009). Proactive strategies to safeguard young adolescents in the cyberspace. *Middle School Journal*, 41(1), 28–34. doi:10.1080/00940771.2009.11461701

Moore, M. (2011, May). Chinese labour camp prisoners forced to play online games. *The Telegraph*. Retrieved from <http://www.telegraph.co.uk/technology/news/8537467/Chinese-labour-camp-prisoners-forced-to-play-online-games.html>

National Crime Agency. (2015, December). *Campaign targets UK's youngest cyber criminals*. Retrieved from <http://www.nationalcrimeagency.gov.uk/news/765-campaign-targets-uk-s-youngest-cyber-criminals>

OPM.gov. (n.d.). Cybersecurity resource center. Cybersecurity incidents. *U.S. Office of Personnel Management*. Retrieved from <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>

Paganini, P. (2016, May). The lucrative but vulnerable gaming industry is ripe for cyberattacks. *Security Affairs*. Retrieved from <http://securityaffairs.co/wordpress/47376/cyber-crime/gaming-industry.html>

Rashid, F. Y. (2013, July). Why video game companies are lucrative targets for hackers. *Security Week*. Retrieved from <http://www.securityweek.com/why-video-game-companies-are-lucrative-targets-hackers>

Richet, J.-L. (2013, June). *Laundering money online: A review of cybercriminals' methods. Tools and resources for anti-corruption knowledge – United Nations Office on Drugs and Crime (UNODC)*. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf>

Seok, S., & DaCosta, B. (2014). Mitigating online threats while promoting scholarship through awareness-raising interventions: A study of young people's technology use, risky online behavior, and literacy of cyber awareness practices. *International Journal of Digital Literacy and Digital Competence*, 5(4), 47–61. doi:10.4018/ijdlcdc.2014100104

Seok, S., & DaCosta, B. (2019). The cyber awareness of online video game players: An examination of their online safety practices and exposure to threats. *International Journal of Cyber Research and Education*, 1(1), 69–77. doi:10.4018/IJCRE.2019010108

Sheridan, K. (2018, September). Cybercriminals launder up to \$200B in profit per year. *Information Week. ITNetwork*. Retrieved from [https://www.darkreading.com/attacks-breaches/cybercriminals-launder-up-to-\\$200b-in-profit-per-year/d/d-id/1331298](https://www.darkreading.com/attacks-breaches/cybercriminals-launder-up-to-$200b-in-profit-per-year/d/d-id/1331298)

Solon, O. (2013, October). Cybercriminals launder money using in-game currencies. *Wired*. Retrieved from <http://www.wired.co.uk/article/money-laundering-online>

Tompkins, T. (2017, September). Fraudsters target video games for credit card fraud. *CreditCards.com*. Retrieved from <https://www.creditcards.com/credit-card-news/how-to-prevent-video-game-credit-card-fraud.php>

Trend Micro. (2015, January). *Data privacy and online gaming: Why gamers make for ideal targets*. Retrieved from <http://www.trendmicro.com/vinfo/us/security/news/online-privacy/data-privacy-and-online-gaming-why-gamers-make-for-ideal-targets>

Trend Micro. (2016, October). *The cybercriminal roots of selling online gaming currency*. Retrieved from <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-roots-selling-online-gaming-currency>

Vincent, D. (2011, May). China used prisoners in lucrative Internet gaming work. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2011/may/25/china-prisoners-internet-gaming-scam>

Weiner, R., & Hawkins, D. (2018, June). Hackers stole federal workers' information four years ago. Now we know what criminals did with it. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/public-safety/hackers-stole-feds-information-four-years-ago-now-we-know-what-criminals-did-with-it/2018/06/19/f42ff2b2-73d3-11e8-805c-4b67019fcfe4_story.html?utm_term=.f41861167c0f

WeLiveSecurity. (2015, July). The 6 biggest online gaming hacks. *WeLiveSecurity.com*. Retrieved from <https://www.welivesecurity.com/2015/07/02/6-biggest-online-gaming-hacks/>

ADDITIONAL READING

Messner, S. (2018, April). How microtransactions and in-game currencies can be used to launder money. *PCGamer*. Retrieved from <https://www.pcgamer.com/how-microtransactions-and-in-game-currencies-can-be-used-to-launder-money/>

National Crime Agency. (2015a, January). *Pathways into cyber crime*. Retrieved from <http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file>

Richet, J.-L. (2013, June). *Laundering money online: A review of cybercriminals' methods. Tools and resources for anti-corruption knowledge – United Nations Office on Drugs and Crime (UNODC)*. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf>

Schreier, J. (2018). *Jason Schreier's posts*. Retrieved from <https://kinja.com/jschreier>

KEY TERMS AND DEFINITIONS

Cybercrime: Criminal activity involving computer systems, networks, and/or the internet.

Data Breach: A security incident involving unauthorized access to data.

Mobile Games: Digitally based games mostly played on mobile devices (e.g., smartphone, tablet) (DaCosta, Seok, & Kinsell, 2015).

Money Laundering: The conversion of illegally obtained money to legitimate money and assets using legal businesses and transfer of currencies.

Video Games: Digitally based games typically played on personal computers or dedicated gaming devices, such as game consoles (e.g., Xbox, PlayStation) or handheld game devices (e.g., 3DS, Vita) (DaCosta et al., 2015).

E-Banking Security: Threats, Challenges, Solutions, and Trends

Fabio Diniz Rossi

 <https://orcid.org/0000-0002-2450-1024>

Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

Rumenigüe Hohemberger

Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

Marcos Paulo Konzen

 <https://orcid.org/0000-0002-8765-970X>

Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

Daniel Chaves Temp

 <https://orcid.org/0000-0002-9724-1331>

Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

INTRODUCTION

There are several types of banks, such as public, private, corporate, development, investment, among other functions, but all have as an essential prerogative the provision of services related to individuals, companies, industries and government money. They range from lending and financing of real estate and vehicles to significant trade-maintaining transactions in the country.

Based on this importance of the banks, security must be applied in the day-to-day of these institutions, because the virtual world is a dangerous place, and without some security control, the tendency is for there to be attempts to steal local money, at the time of looting, among other situations of danger and threats.

Online banking, electronic banking or e-banking consists of the user achieving the most diverse banking operations that are not made within the physical banking agencies. Generally, such transactions are carried out via the Internet, ranging from bank totem to mobile devices.

It has changed people's behavior over the way they spend money since financial transactions can be carried out with just one click. At first glance, this ease and practicality lure the consumers in the sense that their money is safe in and by the financial institution. However, most banking threats are transparent to customers (Singh et al., 2006). It is difficult to quantify the damage of a cyber attack to any financial institution since the impact is not only economic, but other elements make measurement difficult, such as damage to the image and reputation of organizations, loss of confidence in the institution and the loss of potential customers. Therefore, the cost of a cyber attack for an institution may represent a considerably more significant amount than the amount extracted by the attackers.

Although e-banking has been a reality for several years, it is only after 2004 that the incidents began to be reported (Kolodinsky et al., 2004). As a result, e-banking use has declined since threats are reported, but in recent years it has gained strength due to other factors, such as new cryptographic algorithms.

DOI: 10.4018/978-1-5225-9715-5.ch060

None of this is useful when it is the consumer who agrees to be stolen, and this is what most viruses do. Fraudsters take advantage of the innocence of consumers and their inexperience in information security. At the same speed as security techniques advance, threats about such techniques are created (Carminati et al., 2018).

The damage caused by the frauds reaches values in the order of millions of dollars worldwide every year. All these frauds cause customers embarrassment and a lengthy process of adaptation and high costs for the affected banks (Al-Furiah and Al-Braheem, 2009). This chapter, therefore, presents a landscape on all issues ranging from the threat, the challenges to addressing a viable solution to such a threat, and future security perspectives that can prevent new threats from arising that cannot affect online banking transactions.

This chapter presents the following contributions:

- A new taxonomy for classifying threats to e-banking environments.
- A list of new threats that will be organized within the new taxonomy.
- A discussion of such threats and the challenges to address a solution to these threats.
- A review of some trends on e-banking security mechanisms.

From the above, one can note that scams in e-banking environments are not exhaustive, as with each new day a new threat arises. Proposals such as that in this chapter update state-of-the-art concerning new risks and new mechanisms for protecting banking transactions.

This chapter proposes a new e-banking fraud taxonomy, and it presents several types of frauds classified inside such new taxonomy. After, this chapter discusses the advantages and disadvantages offered by the many types of e-banking security proposals. Afterward, we will summarize the work, making it possible to view challenges, trends and future perspectives.

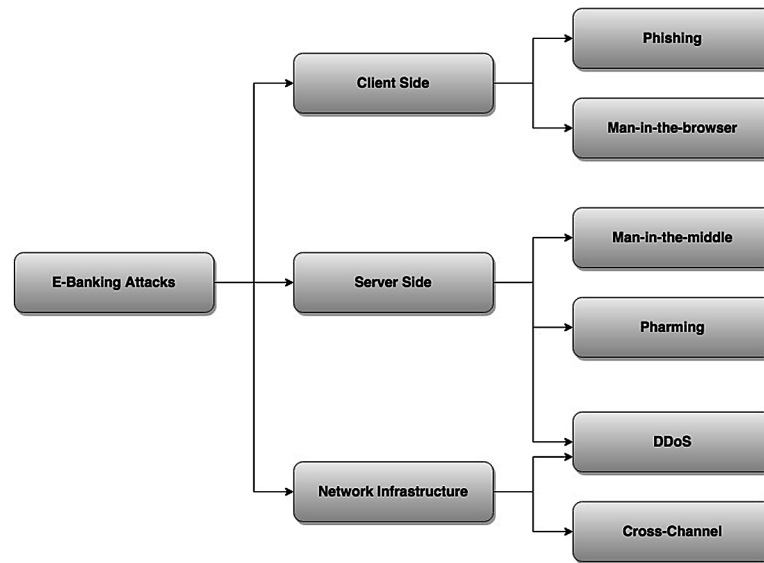
E-Banking Fraud Taxonomy

This chapter proposes a novel taxonomy on security in banking systems, divided into two parts: the first part consists of an approach that organizes and classifies cyber attacks on banking environments, and a second part is an approach that organizes and categorizes current methods of security against cyber attacks discussed in the first part of the taxonomy.

The evolution of computing and new technologies has changed the way data manipulation and information have undergone various changes. As for money, online banking has emerged to make life easier for people, bringing added convenience and agility to the day-to-day operations of our daily activities. Checking balances, transferring amounts and making purchases over the internet is a reality today, but many people still have a bit of a fear of doing this.

Figure 1 shows target-based cyber attacks. Therefore, the attack can be directed to the client and its devices and applications, to the server that supports the banking service and receives client requests, or attacks on the communication between client and server. Threats directed at client devices or applications are mostly idealized through viruses or their variations and require some form of client acceptance (implicit or explicit). Threats to servers or infrastructure that supports banking services are less frequent but usually, occur through cloned services. Threats over the communication infrastructure between clients and the server usually occur through redirecting the network flow to fake sites.

Figure 1. Taxonomy of e-banking attacks, divided by attack target



Based on the increase in the reporting of scams and losses, the fear becomes even more significant, causing many to isolate themselves from this technology and its facilities. However, with some simple procedures, we can make these operations more reliable.

Figure 2 presents proposed solutions to avoid most attacks fanned in the first part of this taxonomy. Such protections can be divided into physical mechanisms and devices or virtual systems and environments. Banking security by physical means has increased in recent years, as it attempts to individualize access, based on devices that are only in property of the client or based on biomarkers. Virtual security consists of digital systems that create abstraction or security mechanisms over which the client can send their data securely.

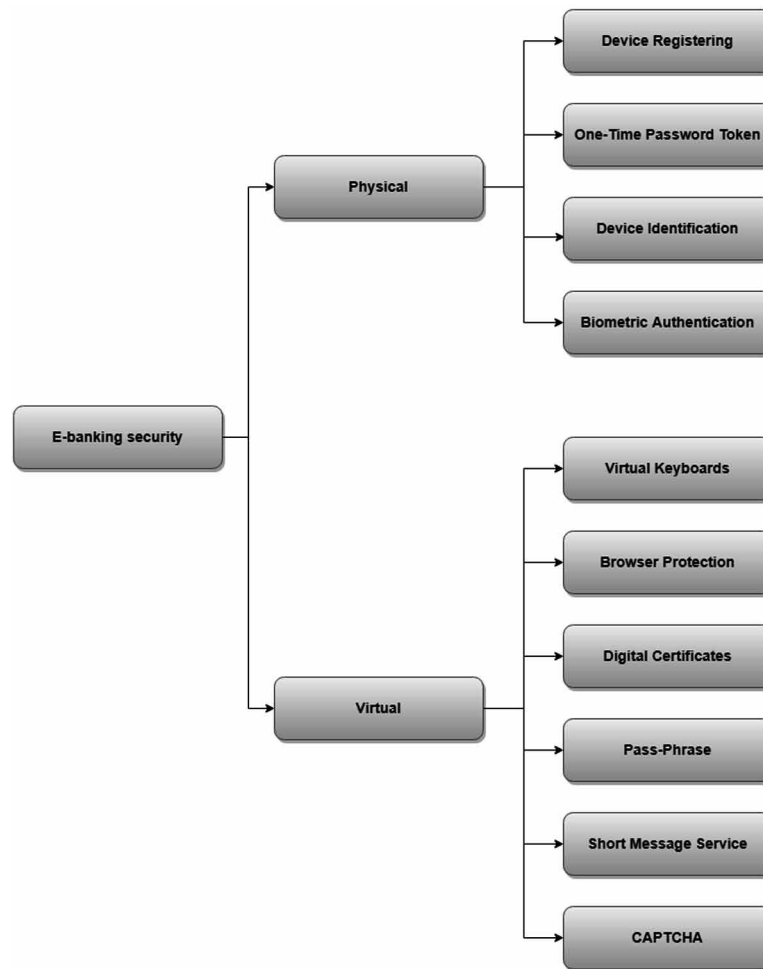
However, while banks are committed and invested in protecting their virtual boundaries against known and unknown threats, preserving the full breadth of existing IT infrastructure is not an easy task. The large, dynamic threat environment, coupled with the challenge of improving customer safety habits, gives the fraudsters even more vulnerabilities to attack.

The scenario in which the most diverse financial institutions are inserted is also characterized by the need for well planned, integrated, fast, functional and, above all, secure insurance networks. As you can imagine, managing the network of a large corporation, especially in the financial sector, is a complex task. Based on the above, in this chapter, we will describe and classify the different attacks, security challenges, and trends according to the proposed taxonomy.

E-Banking Threats

ISO/IEC 27002 (ISO/IEC 27003, 2013) defines information security threat as being an agent that may cause an incident in a computer system, likely to result in harm to an organization or individual. Threats can compromise systems by exploiting one or more vulnerabilities, whether technological or social vulnerabilities.

Figure 2. Taxonomy of bank security mechanisms divided into physical and virtual



A threat can result in a security attack or incident and occurs as a result of a threat that exploits one or more vulnerabilities. The attack is the absolute fact caused, generating, in most cases, financial or image damages.

In e-banking, threats can mean financial impacts on individuals and banking organizations, as well as reputation impairment. We outline the critical threat methods and tools that put e-banking services at risk.

Phishing. It is a type of attack that aims to steal electronic credentials or financial information from an individual. Usually employs the use of false pages or links, combined with social engineering. The main methods used are fake e-commerce or e-banking pages, fake links shared on social networks, e-mail messages containing links to malicious code pages or electronic forms that solicit personal or financial data. Regardless of the method used, the attackers try to induce the user to click on malicious links using social or economic appeal messages (Montazer and Yarmohammadi, 2013). Phishing attacks are often used to steal information from online payment systems or e-banking access information. For example, the user may receive an alleged message from his bank requesting an update on his/her registration, under penalty of cancellation of his account and a link of a false electronic form is informed. By completing your information on this form, the data is sent to a malicious third party (Hewamadduna, 2017). Different types of attacks and techniques perform phishing, such as:

- **Malware:** They are programs specifically designed to perform harmful actions and malicious activities on a computer. When installed on your computer, malicious code will have access to sensitive data stored on the device and may perform operations on behalf of users. The main types of malware are Botnets, Keylogger, Screenlogger and Trojan-Banker (Méndez-Garcia et al., 2014). The use of malware to capture user banking information is the most widespread type of attack due to the diversity of malicious code and the full range and potential of device infection.
- **Keylogger:** It is a type of malware capable of capturing and storing user-entered keys on a computer keyboard. Its activation, in many cases, is conditioned to a prior action of the user, such as access to a specific e-commerce site or Internet Banking (Wazid et al., 2013) (Sbai et al., 2018).
- **Screenlogger:** Similar to the keylogger, able to store the position of the cursor and the screen displayed on the monitor, at times when the mouse is clicked, or the region that surrounds the place where the mouse is clicked. It is a method widely used by attackers to capture keys typed by users on virtual keyboards, mainly available on Internet Banking sites (Sbai et al., 2018).
- **Trojan Banker:** Collects user's bank details by installing spyware programs that are activated when Internet Banking sites are accessed. They are often disguised as authentic software, but when run monitor and capture user data.
- **Sniffing:** It is a technique that consists of inspecting the data transmitted in computer networks, through the use of specific programs called sniffers. This technique can be used by attackers to capture sensitive information such as passwords, credit card numbers, and the contents of confidential files that are traveling through insecure or weakly encrypted connections (Muhammad et al., 2016).
- **Social Engineering:** One of the primary methods for obtaining confidential information from users. The fraudster uses social engineering to deceive and persuade potential victims to provide sensitive information or to take action, such as executing malicious code or accessing fake pages. In the context of e-banking, it is combined with the Phishing technique to steal logins, passwords or credit card numbers (Suleimanov et al., 2018).

Man-in-the-Browser (MITB): It is a type of attack similar to MITM, but in this case, a Trojan is used to intercept and manipulate calls between the web browser and security libraries, such as encrypted connections. It is a type of attack challenging to be perceived by ordinary users since it can handle e-banking transactions even when security factors are in use (Alghazo and Latif, 2017).

Man-in-the-Middle (MITM): Attack technique that is based on exploiting existing vulnerabilities in communication between two points. Its focus is on intercepting the traffic resulting from the communication of these two, acting as an intermediary. The intermediate can be inserted transparently or through an infected device (Ngalo et al., 2018). The method called sniffer is used to listen to the network, allowing the capture of desired packets. As an example of devices that can be compromised by MITM, we can mention the home wireless routers.

Pharming: Also known as DNS cache poisoning or DNS spoofing, it is a type of MITM attack that compromises the security of name resolvers on the Internet by introducing false information into the DNS server cache, causing the DNS server to return an incorrect IP to a query a web page, diverting traffic to a malicious computer. One of the primary targets of a DNS Spoofing attack is the home routers and DNS servers of local networks (Hussain et al., 2016). Pharming is widely used as a method for phishing attacks. For example, the user attempting to access your e-banking page will be redirected to a fake page that can be used to collect user data, such as access passwords.

DdoS: Distributed Denial of Service is when a set of computers is used in the attack to de-operate a service, computer, or network connected to the Internet. People or institutions that depend on the affected resources are impaired, as they are unable to access or perform the desired operations as financial transactions, for example (Wahab et al., 2017).

Cross-Channel: It is an advanced attack method in which the fraudster steals the credentials and personal information of a user of a service to commit fraud on an associated channel and account. Cybercriminals use advanced attack techniques to exploit vulnerabilities in a channel to steal personal information from other related channels. This type of attack can be combined with social engineering techniques (Khande and Patil, 2014). In general, such type of attack can use botnets. It consists of infected computer networks that can be controlled remotely to attack other computers or systems. An example of how Botnets can compromise a banking system are DDoS attacks, in which a network of infected computers can trigger a mass attack on a server or network infrastructure of a bank (Sood et al., 2016).

E-Banking Security Challenges

As more and more users use electronic banking for bill payment, wire transfers, and e-commerce, malicious users are eyeing that slice of customers that may be exposed to attacks if banks fail to take preventive measures.

In 2017, Brazil already had 940,000 fully digital accounts in the country, and 76% of Brazilians use internet banking services, thus, just as banks have for years invested in safer coffers to maintain except in today's prime security is a factor of advantage over the competition. In addition to scratching the image of the bank, it is inadmissible for a company to lose space for the competition if it does not have consistent security and also pass this image of confidence.

In this chapter, the challenges and defenses that banks have for security have been classified. The classifications are like "Physics", where these are not included in the system of the bank and the "Virtual", that are in the site/own system of the bank. In many cases, banks use more than one security method to increase efficiency and trust in users' access.

Device Registering: Security method in which the bank recognizes and registers the user equipment (Peotta et al., 2011). Usually, this registration happens physically in the agency or the first virtual access to the account. After this, only equipment registered by the bank has access to the account and its transactions.

One-Time Password Token: A token is an electronic device with the ability to generate passwords based on time synchronization (Wayman et al., 2005). The device has a button, where pressed, will display a numeric key, where the user will use as a password. Generally, this method is used as a second instance of security, shortly after the user enters his/her password. Another form of protection similar to One-time Password Token is the One-Time Password Card (Wayman et al., 2005), which consists of a card containing a table with two fields: sequence number (position) and key number. Each card can provide up to 70 sequential numbers. Its operation consists in the bank requesting the key from some random spot, thus confirming the authenticity of the transaction (O'Gorman, 2003).

Device Identification: In this security feature, information about the device, such as operating system, IP range, cookies, etc., is collected to allow access only to legitimate equipment and also to prevent suspicious access, such as from a country other than user resides (Peotta, 2011).

Biometric Authentication: In this example of authentication, stable body characteristics such as digital, iris, face, and palm are used (Wayman et al., 2005). After scans, these data are compared with those already registered in the system and after that, authorizing or not accessing the site or continuing the banking operation. This method is often used together with the user's password (Von Ahn et al., 2003).

Virtual Keyboards: The use of virtual keyboards for entering bank passwords is a method where the user instead enter the information via a keyboard, will use a keyboard on the computer screen and the mouse for this (Rajarajan, 2014). This method arises to prevent keyloggers from capturing the password entered via the keyboard. Generally, the positions of the letters and numbers that appear on the screen for the user are random, thus avoiding the capture of the password by programs that record the location of the user's mouse (Von Ahn, 2003).

Browser Protection: In this method, the bank itself provides software to protect the user's browser (Peotta, 2011). Usually, this installation happens at the first access to the account and is done automatically and making the user's access impossible without this installation being made.

Digital Certificates: In this method, the digital certificate is a document that proves the identity of a user or company, issued by a certifying entity. At the moment the user accesses the bank's website, this certificate is checked, verifying that the site belongs to the bank (Wayman et al., 2005).

Pass-Phrase: This method differs from the already known password and is widely used as a second authentication method. Passwords are used for access to bank accounts and consist of only one word, containing letters, numbers and symbols and a reduced size. Passwords are phrases that, besides including the same letters, numbers, and symbols of the passwords, can also contain spaces and even a larger quantity of characters, making it difficult to break this information. Generally, pass-phrases are used as a second authentication method (Peotta, 2011), only to confirm the transaction.

Short Message Service: This method consists of a notification to the user who owns the bank account (Peotta, 2011). For each transaction, a message is sent to the owner's cell phone informing about the type of transaction and the value. If the recipient does not recognize the transaction, it is possible to block the card by replying to this message. Some banks also use this method for a second confirmation before the transaction takes effect. The user receives a verification code and will have to enter the code received at the moment the system requests.

CAPTCHA: This is a program, where through tests, be these images, texts or simple mathematical equations can differentiate that humans or machines are doing the access to the site (Von Ahn, 2003). The primary purpose is, if the access to the bank is made by malicious software, this software will not be able to respond to the CAPTCHA test, thus evidencing an attack.

E-Banking Security Trends

The need to remain competitive forces banks to offer new services and amenities. Also, the adoption of new technologies can also bring risks to banking activity. Below we describe some of the challenges we consider essential for E-Banking security:

- **Trust:** One of the highest qualities sought in a financial institution is reliability because it is given custody over immense amounts of values (ISO/IEC 27002, 2013). If a bank suffers an attack and can not defend itself, its image before the users can be compromised.
- **The Resistance of Users:** People are resistant to significant changes by nature. Therefore, users can be resistant to major modifications, resulting in insecurity. We can cite as sudden changes the digital banks (Sood et al., 2016).

- **User:** The development of services for e-banking can be done through software engineering techniques, regulations of sector entities or government agencies among others to ensure security. However, the device used by the user and how it is used can compromise all efforts made. The use of malicious or malware-infected software or Keyloggers can capture sensitive information, weakening security efforts. Another technique that can be used is Social Engineering, which is one of the most difficult to prevent. In order to minimize such vulnerabilities, it is essential to educate the user, use overlapping authentication methods and identity verification mechanisms.
- **DDoS:** Annoyance for not being able to perform a transaction can cause damage to a bank's image, affecting user confidence and causing loss. The DDoS attack directly targets the unavailability of services. This can cause a bank to have several of its services severely affected. For this, there is a need for containment plans and mitigation of the attack.

Trying to attract customers confidence, new technologies and services are proposed. In the financial sector, it is no different — the need to remain competitive and attractive means that banks increase the number of existing solutions and services. One of these is called fintech - companies or startups aimed at the financial and technological sector, with the aim of creating and exploring old services in a remodeled way or even building new services. Examples of Fintechs are Paypal, Nubank, SoFi, and Vérios. Other areas of interest can be cited:

Mobile: With more and more people using smartphones there is a migration of services to these devices, seeking to take advantage of the characteristics of these devices (Peotta, 2011). The availability of secure applications for access to banking services will be a challenge, as the number of users catches the attention of criminals.

Bank 3.0: Taking advantage of the digital niche, digital banks arise as an alternative to physical banks. The main difference lies in their organizational structure. They have a centralized architecture and no branches, however, due to the medium where they are inserted - digital, cover a large area of coverage. As your challenges arise: 1) Need to be reliable and credible; 2) Offer competitive and safe services since the entire business model is developed on the Internet.

Biometry: Biometric identification comes as an alternative to conventional authentication methods (passwords and codes), because it combines several desirable characteristics for security, being: the user can not forget the low cost, reliability, not vulnerable to some social engineering techniques, the speed of authentication. Today, biometrics multispectral image sensors are enabled for encryption and hardware tampering - which protect not only the integrity of the sensor but also the communication between the client and the sensor. It is a feature highly valued by the market since these sensors are five times more accurate and four times faster in ATMs and multibank, with a significant reduction of errors. In general terms, there is a gain regarding performance and interoperability. For this reason, in addition to the financial system, the new line of biometric authentication has been adopted in health, electoral and governmental systems.

BlockChain: It is a technology organized in a decentralized way for the storage and measurement of records. Security is inherited from the various decentralized nodes with the power to issue and authenticate records. Thus, any record to be stored can be verified and validated, not by one but by several bases. This record should only be included in the database if it is authorized by several databases, thus increasing security. Many Fintechs were founded and are dedicated to the study and improvement of the use of Blockchain as Circle of Goldman Sachs, Quorum division of JP Morgan. The main difficulties of its adoption are interoperability, privacy, and encryption.

Artificial Intelligence: Considered as one of the primary resources to modify the operation of the banks, its area of coverage goes through the manipulation of the user experience, automation of tasks, identification of anomalies. There is also the risk that this technology will be used by criminals to create intelligent and dynamic tools to be used in fraud.

Major bankers are already testing (in partnership with mobile operators) payments via NFC (Near Field Communication) with mobile phones. This approach payment technology has been used for years in countries like Japan and Australia, but it is still new in several countries. Contrary to what many consumers imagine, these electronic payment devices take over the same logical and physical security mechanisms used by traditional credit cards. And more than that, they offer additional layers of security, reducing the chances of cloning or illegal purchases by third parties, even if the customer's smartphone has been stolen.

In this area, it is worth mentioning that one of the most significant cybersecurity challenges for the banking sector in 2018 is not to implement the technology, but rather to convince the trader that these disruptive payment methods are safe. And they are.

Another exciting technology of online payments that promises to reduce the rate of thefts is the virtual card. These cards are generated by internet banking (provisional security codes) for use in a single purchase. After that, if someone has access to the data, it will not be able to complete the transaction, since all the encoding has already lost its validity. These new technologies have been redesigning the concept of cybersecurity in the country.

The greater the interaction, however, the higher the risks, since these advances also reach cybercriminals. A market has emerged not only from displays of malicious code but also from complete malware offerings such as a service, threat kits, and attack service providers. Now, intruders can buy or outsource complex highly evasive multi-step attacks with little investment or almost no experience, which reduces the entry barrier of new hackers into the market.

Therefore, layered security should be the strategy for new implementations, i.e., it is essential to use different controls at different points in the process of each transaction. This approach is vital to enabling banks to become even more cyber-resistant: also if a defense is circumvented, there will be others to ensure the integrity of the entire ecosystem.

Multilayer security not only allows banks to eliminate the idea of security as an impediment but also to leverage security as an element that enhances differentiation and business innovation. In this way, banks can adapt more flexibly to competitive and emerging threats and opportunities.

FUTURE PERSPECTIVES

Banking institutions will face significant challenges regarding security and innovation from now on. Every day, a growing number of processes move to the digital world, which implies a change in mentality, business models and therefore also in security measures. Customers, faced with this move, expect to be positively surprised by the services of their banks. This expectation can be translated into four words: multichannel, fluency, simplicity and innovation. Avoiding lengthy, complex processes that depend on the physical presence of the client in a bank branch can even encourage them to demand new banking services. It can be, for example, an integrated application for mobile phones, tablets, smart watches, and wearable devices. Or, who knows, a multi-channel experience that flows smoothly, keeps the client engaged and encourages more frequent interaction with the institution.

The idea of E-Banking has been consolidated for some time, not only by the advance of the Internet but also becoming present with the help of innovation and the technologies used for information security. The eternal paradox of information security is that with every new technology that comes to generate customer convenience, it also produces some trace of vulnerability that at some point will be used by cybercriminals to invade systems, steal or hijack sensitive data. Talking about the future of financial institutions, makes us think about how we evolve in different ways. While for banks targeting Internet Banking, Mobile Banking and even BitCoin are common, we can also associate this evolutionary leap in encryption, digital signature, data protection, Blockchain, and various other security-related terms.

Technological developments have pointed to an increasingly digital future, and financial transactions are being incorporated into our routines as something more simplified and transparent. We can see this reality through payments made with mobile and wearable devices. The financial sector has always been one of the most advanced regarding investment in IT and products and services related to financial transactions, and it is no wonder that the emergence of Banks 3.0 comes from technologies such as cloud computing and cybersecurity.

It is noteworthy that this evolution came from a disruption of paradigms, the rise of digital banks represented one of the biggest challenges for the financial market, where it fostered significant changes in the behavior of its consumers. It is possible to see soon that we will have a significant conceptual change regarding financial institutions, in the era of Banks 3.0, they cease to be banks and become financial assistants, all happening online and with little interference from people or institutions regulatory frameworks.

The significant shift from traditional to digital banking has its base formatted in efficiency and confidence through technology and cybersecurity. A digital banking experience, the essence of the Banks 3.0 concept, will be driven by the most automatic, intelligent and secure delivery of products and services. But to consolidate this new concept of bank information security will be fundamental. CEOs who intend to offer this unique experience, in the future so present, besides understanding about the new business models, processes and technologies that will allow us to evolve to the concept of Bank 3.0, should consolidate the idea that without security investments this will not be possible.

Ultimately, Bank 3.0 needs to be agile enough from a technological, structural and cultural standpoint to allow it to adapt to rapidly changing business and technology environments continually. A significant challenge when integrating so much technology and security, identity and compliance requirements. Therefore, the basics that an organization must consider to be increasingly protected are related to processes, staff, and technology. It consists of the application of measures with different approaches, from operational, administrative, technical or technological, to legal and regulatory issues. Only taking all this into account, an institution will have a full possibility to guarantee its security in the face of the many adversities that currently exist in the corporate environment.

REFERENCES

- Al-Furiah & Al-Braheem. (2009). Comprehensive study on methods of fraud prevention in credit card e-payment system. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services (iiWAS '09)*. ACM.
- Carminati, M., Polino, M., Continella, A., Lanzi, A., Maggi, F., & Zanero, S. (2018). Security Evaluation of a Banking Fraud Analysis System. *ACM Trans. Priv. Secur.*, 21(3). doi:10.1145/3178370
- Hewamadduma, S. I. (2017). Detection and prevention of possible unauthorized login attempts through stolen credentials from a phishing attack in an online banking system. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. 10.1109/ICRIIS.2017.8002440
- Hussain, M. A., Jin, H., Hussien, Z. A., Abduljabbar, Z. A., Abbdal, S. H., & Ibrahim, A. (2016). DNS Protection against Spoofing and Poisoning Attacks. *Information Science and Control Engineering (ICISCE) 2016 3rd International Conference on*, 1308-1312. 10.1109/ICISCE.2016.279
- ISO/IEC 27002:2013. Information technology -- Security techniques -- Code of practice for information security controls.
- Khande, R., & Patil, Y. (2014). Online banking in India: Attacks and preventive measures to minimize risk. *International Conference on Information Communication and Embedded Systems (ICICES2014)*. 10.1109/ICICES.2014.7033940
- Méndez-García, V., Jiménez-Ramírez, P., Meléndez-Ramírez, M. Á., Torres-Martínez, F. M., Llamas-Contreras, R., & González, H. (2014). Comparative analysis of banking malware. *IEEE Central America and Panama Convention (CONCAPAN XXXIV)*, 1-5. 10.1109/CONCAPAN.2014.7000412
- Montazer, G. A., & Yarmohammadi, S. A. (2013). Identifying the critical indicators for phishing detection in Iranian e-banking system. *The 5th Conference on Information and Knowledge Technology (IKT)*, 107-113. 10.1109/IKT.2013.6620048
- Muhammad, L. Q. (2016). Android Mobile Banking Application Security from Reverse Engineering and Network Sniffing. *International Journal of Computer Science and Information Security*, 14(10), 461.
- Ngalo, T., Xiao, H., Christianson, B., & Zhang, Y. (2018). Threat Analysis of Software Agents in Online Banking and Payments. *IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, 716 - 723. 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00125
- O'Gorman. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12), 2021-2040.
- Peotta (2011). A Formal Classification of Internet Banking Attacks and Vulnerabilities. *International Journal of Computer Science and Information Technology*, 3(1), 186-197.
- Sbai, H., Goldsmith, M., Meftali, S., & Happa, J. (2018). A Survey of Keylogger and Screenlogger Attacks in the Banking Sector and Countermeasures to Them. In A. Castiglione, F. Pop, M. Ficco, & F. Palmieri (Eds.), *Lecture Notes in Computer Science: Vol. 11161. Cyberspace Safety and Security. CSS 2018*. Cham: Springer. doi:10.1007/978-3-030-01689-0_2

- Singh, S., Cabraal, A., & Hermansson, G. (2006). What is your husband's name?: sociological dimensions of internet banking authentication. In *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments (OZCHI '06)*. ACM. 10.1145/1228175.1228217
- Sood, A. K., Zeadally, S., & Enbody, R. J. (2016). An Empirical Study of HTTP-based Financial Botnets. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 236–251. doi:10.1109/TDSC.2014.2382590
- Suleimanov, A., Abramov, M., & Tulupyev, A. (2018). *Modelling of the social engineering attacks based on social graph of employees communications analysis*. In *IEEE Industrial Cyber-Physical Systems*. St. Petersburg, Russia: ICPS.
- Von Ahn, L. (2003). *CAPTCHA: Using Hard AI Problems for Security*. Springer Berlin Heidelberg.
- Wahab, O. A., Bentahar, J., Otrok, H., & Mourad, A. (2017). Optimal Load Distribution of VM-based DDoS Attacks in the Cloud. *IEEE Transactions on Services Computing*.
- Wayman. (2005). An Introduction to Biometric Authentication Systems. *Biometric Systems*, 1-20.
- Wazid, M. (2013). A framework for detection and prevention of novel keylogger spyware attacks. *2013 7th International Conference on Intelligent Systems and Control (ISCO)*. 10.1109/ISCO.2013.6481194

E-Banking Frauds: The Current Scenario and Security Techniques

4

Sandal Azhar

University of Delhi, India

Manisha Shahi

University of Delhi, India

Vikas Chhapola

University of Delhi, India

INTRODUCTION

Electronic banking or net banking includes any electronic payment system that permits clients of a bank to make transactions through the bank's internet-enabled website or app. It gives access to the facilities of the banks online if there is a required means for it. It provides various services like funds transfer, payment of bills, checking of account details, online shopping and recharge. E-banking has found its place in daily lives as it works as per the comfort and convenience, provides faster transactions, is cost effective and can be done from anywhere. With these advantages, it is also becoming a centre of attraction for Cyber frauds- online frauds in which a person's account is used to transfer funds for financial gain. The Cyber criminals make easy money by duping users, by methods like phishing, vishing (voice phishing), making people download Trojans and malicious softwares which can provide their credentials to the criminal.

E banking frauds have become the most common kind of Cyber frauds which is gaining high popularity. According to a global survey conducted by FIS, a financial services technology firm, Indians are among the most frequent victims of online banking frauds. (Jain, 2018). In comparison, only 8% of people from Germany reported a fraud followed by 6% in the UK. This scenario demands a high level of security measures using latest technology which the Cyber criminals cannot circumvent.

This paper aims at reviewing all types of banking frauds and the measures which should be taken at the bank as well as user level for maintaining the integrity of the online banking systems. It also studies about current scenario of security that is being implemented by the banks and the potential areas like machine learning and big data analysis which can be used as a tool to combat the plight of this blooming industry. The research also directs towards different cases of frauds globally, their cause and implications. It also provides an insight in the study of fraudulent certificates, the damage it causes, and the suggested certificate transparency phenomenon which can solve this problem.

The main focus of the study is to mention the emerging techniques of security that have the potential to combat this menace of e banking frauds. Certificate transparency, HTTP Security Response Headers Automated Analysis Tools, Behavioural analytics and Big Data can help us build systems that are secure against these attacks.

DOI: 10.4018/978-1-5225-9715-5.ch061

BACKGROUND

Online banking today is so prominent that it is hard to imagine that it was not far ago that this boon came into existence. The beginning of online banking dates back to as early as 1980s when biggest banks in New York started providing their customers home-based services. Customers could access their bank accounts to view statements and pay bills. However, the real breakthrough in internet banking arrived in mid 1990s when internet was acknowledged as a distribution media with great potential. The ease and comfort that this breakthrough brought with itself was commendable and life changing. While this mode of access to the banks and ease of handling the accounts was very convenient and had great potential, people soon realized that this flexibility came at a price. Cyber criminals started considering potential in e-banking to accomplish their vicious motives of financial gains by hacking into the systems. Conventional methods of banking frauds soon were replaced now by e-banking frauds. Technological innovations that the banking sector adopted in their quest for growth, in turn opened a gateway for higher levels of cyber risks. It probably introduced new vulnerabilities and complexities into the system. Hackers are now exploiting these loopholes or finding and inventing new technologies to find such vulnerabilities in the banking systems. Various studies and work have been directed towards this critical topic of online banking frauds. Research on this topic includes both the preventive security measures, strengthening the system and the detection of frauds. Banks are constantly working towards the enhancement of security and using various methods to keep the system safe, like encrypted channels for the transactions, two factor authentication and many technologies are being worked upon to secure the system from being exploited by the criminals. Data analysis software are used by examiners to analyse a bank's business data to gain insight into how well internal controls are operating and to find transactions that indicate fraudulent activity or the risk of fraud.

As the security measures on the bank's side tighten so do the advancement in technologies on the hacker's part, as they keep themselves a step ahead. So, this is a need of the hour to work and research in this direction of developing security measures which are technology at par with the technologies used in these cybercrimes. This industry needs more and more cyber security specialist and passionate minds that want to work for the security of online banking systems and find counter measures for all possible attacks on internet banking. Current research aims at reviewing E-banking frauds scenario as a whole, all kinds of attacks on the banking systems, the techniques used behind them and their potential preventions.

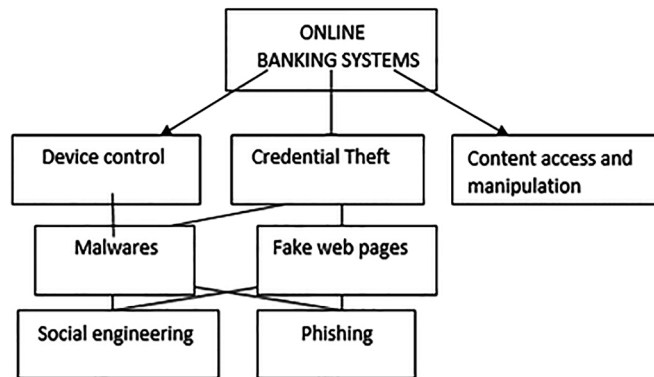
CURRENTLY ACTIVE COMMON ATTACKS:

This section first describes the basic model or nature on which the attacks are based on and the study goes on to explain the techniques currently active in deploying the attacks.

NATURE OF ATTACKS:

In this era where the demand for online transactions is growing at a very rapid pace, we need to have complete technical knowledge of the attacks that are committed online and the vulnerabilities they are based on, to provide appropriate security measures and the solution to the growing problem of e-banking frauds. Attacks are escalating their range and complexity to levels that need high technical understanding on the part of its developers. Every attack is determined to defeat in one way or the other, the authenti-

Figure 1



cation systems used by banks to their customers to function. These attacks are based on software tools made by the hackers, applications running on web environments, either in the computer of the victim (malware) or by using various social engineering ways to attract victims to a fake website (Phishing), or on their mobile devices by downloading rogue applications (false APP) (Vilà, 2015)

Figure 1 (Holtz, David, Deus, de Sousa Junior, & Laerte, 2011) explains the main vectors on which the attacking techniques can be based on:

1. **Credential Theft:** This is the most common attack wherein the attackers try to get the user credentials by using malwares or phishing, so as to login as legitimate users and carry out the financial transactions.
2. **Device Control:** It is more complex where the attackers takes full control of a device instead of stealing the credentials from authentication process, and then the user's device itself is used to access the online banking and commit fraud.
3. **Content Manipulation or Man in the Browser Attack:** Occurring in the application layer between the user and the browser. Without the awareness of the user, the attacker can modify and manipulate data.

TECHNIQUES OF ATTACKS:

Most of the attacks are being performed by tools which are nowadays easily available on web. These tools can capture sensitive information and are even capable of replacing the authentic website page with a fake one and the user is made to input on that fake site. Here are some types of common attacks which break the security of the banking systems:

1. **Malwares:** In the present Internet-connected society, e-commerce and e-government (e.g. e-banking and e-payment systems) are being extensively used. Such systems and services can and have been targeted by cyber criminals, and malwares like banking Trojans are popular among financially motivated cybercriminals. For example, a cyber-attack in South Korea allegedly saw 32,000 computers belonging to broadcasting organizations and banks infected with a malware that overwrote the Master Boot Record (MBR) (Kim, Kim, & Park, 2014). Then, in 2013, the Crypto-Locker ransomware reportedly infected around more than three million machines, causing more than 6

million USD worth of damages (Lee, 2013). A more recent case was witnessed in Bangladesh, in 2016, which was a \$951m raid on Bangladesh's central bank where the security systems were penetrated by a criminal gang of hackers with malware that cloned legitimate transactions (All about digital banking fraud prevention).

Malwares can be broadly categorized in aspects like network based and those that aren't network related (Saeed, Campus, Selamat, Ali, & Abuagoub, 2013), and further divided into adware, spyware, virus, worms, backdoors, rootkits and Trojans (Saeed, Campus, Selamat, Ali, & Abuagoub, 2013) (Zolkipli & Jantan, 2011) (Zolkipli & Jantan, 2010) (Kiyavash, Koushanfar, Coleman, & Rodrigues, 2013) (Singh, Singh, & Joseph, 2008) (Salomon, 2010). One important class of malwares that is being extensively used in e banking frauds are trojans.

- a. Trojans have many ways of working, depending on the design they may facilitate/performance capabilities like backdoor, sniffing, spamming etc.

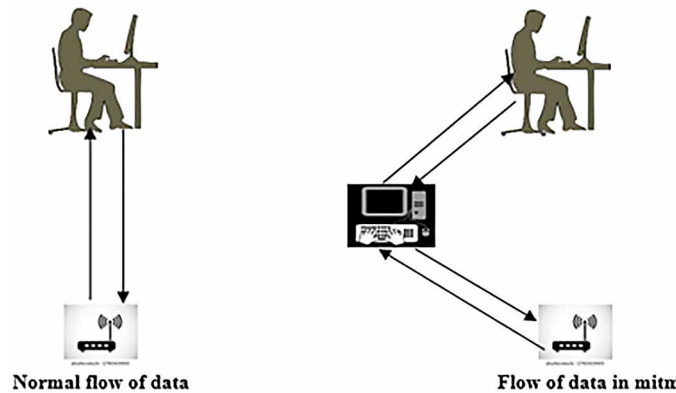
Trojans are considered as one of the most persistent malwares that can evade conventional firewall and antivirus capabilities over a noteworthy period allowing attackers to harvest sensitive information. (Hutchins, Clopp, & M. Amin, 2011)

They pose to be one of the most major threats for the security of e-banking because they are purposely developed to execute frauds in banking systems. The banking Malware (Trojan) is a code that is installed on the user's computer using standard techniques of computer viruses and worms, for capturing data (including information of authentication and user operation and sensitive information like credit card details) exchanged by the user and his bank when the victim uses internet banking. The most fundamental are the "key loggers" that gather, record, read the user's keystrokes or capture images even displayed on the screen when the user operates the banking website (Vilà, 2015). The key loggers keep a track of user's activities on the website.

The Malicious codes continue specializing. Banker Trojans are modified exclusively for banks, changing the look of your real website, by superimposing a fake window when the user accesses the online service of your bank. The overlay looks alike to the legitimate website so that the user enters information authentication codes in it, believing that they are giving the details in the real website. One of the biggest threats that banks are presently facing is the SSL invading Trojan Horses which bypass the secure and authenticated tunnel mechanisms that are the safety backbone of today's internet banking and financial institutions. Trojan horses that the hackers have lately devised have become more complicated as banks have increased their online security measures. Earlier, such malwares could just take usernames and passwords for specific banks, but the hacker had to manually access the compromised account to withdraw funds. Cyber Criminals have now come up with exceptionally sophisticated tools in order to hijack money from the online banking systems.

2. **Man-In-The-Middle Attack:** Normally, the hacker who may control network routers or switches, Wi-Fi access points, and/or DNS is capable to lure the users by disguising their identity (e.g., through DNS poisoning) and it appears as if the data was coming from a trusted source. So instead of going to the legitimate website, users don't realize that they actually used the fraudster's website. The information provided by the victim during the session will be captured and sent to

Figure 2.



the attacker, who can then use the information for committing financial frauds. These attacks can be done using fraudulent certificates which make the user think that the website they are logging into is secure and legitimate without realizing that the SSL certificate of the attacker's website is fake. (Georgiev, et al.)

Figure 2 describes the scenario of a man in the middle attack where the first case depicts the normal flow of information between the server and the client and the second case explains the attack where the invader sits between the client and the server and all the information flows through him.

3. **Brute Force Attacks:** This is a technique where the attacker, with the help of a software tries to break the security and gain access to messages, user ID's, and passwords. In brute force attacks, automated softwares are used to generate many guesses to reach the desired data. It is a kind of trial-and-error method for guessing the passwords of the victims.
4. **Phishing:** It is a deceiving technique which involves social engineering (that refers to psychological manipulation of people into performing some actions or revealing confidential information) and technical subterfuge (Security engineering: a guide to building dependable distributed systems (2nd ed.), 2008). Sensitive information such as usernames, passwords, credit and debit card details are retrieved, as a legitimate looking email or website turns out actually to be a spoof. Victims of this fraud are typically cajoled by certain sources which purports to be genuine such as social websites, auction websites, banks, online payment platforms (safe-browsing-protecting-web-users-for.html,n.d.). Phishers have started Using Encryption to Fool Victims from July 2018, when Google began labelling non-HTTPS websites as "Non-Secure" in the Chrome browser as HTTPS indicates secured interaction between a browser and the website that the user is surfing. HTTPS is recommended on the websites that include online sales or password-protected accounts. Phishing Activity Trends Report, 2nd Quarter 2018 by APWG. APWG member Mark Monitor observed rise in the number of phishing that aimed web mail providers, soaring to 21 percent of all phishing attacks in 2Q 2018, up from 18.7 percent in 1Q 2018 (APWG Phishing Attack Trends Reports, October 20, 2018.).

5. **Fraudulent Certificates:** Fraudsters create sites mimicking the original websites by deceptively issued security certificates to dupe customers into offering over their details (Fake-banking-sites-wrongly-issued-with-authentication-certificates.html, n.d.). Cybercriminals can now steal money by taking gain of the one safety measure every Internet user has been taught to trust: the green padlock in web browsers. These padlocks are supposed to indicate a reliable digital certificate is in use, but now bad actors can attain them for free. The posting of fraudulent certificates does not essentially mean that the entitled operator or certifying agent was involved in illegitimate activity. They may have been shaped and used without the operator's consent or the certifying agent of the certificate (www.ams.usda.gov/services/enforcement/organic/fraudulent-certificates, n.d.). This deceiving technique is taken care of, by the Google's Certificate Transparency project which has been discussed further in the article.

Presently online banking frauds tops the cybercrime lists in many countries worldwide. So, it is a critical time that our banking security and authentication techniques should be at par, in fact a step ahead of the sophisticated tools and technologies the cyber criminals have been developing to crack our systems. The E-banking systems should have efficient security procedures which are able to identify users precisely and then permit the transactions, thus extenuating fraud. Two main factors of the identification schemes: unique secret information earlier shared by the customer and the bank "passwords" and exclusive characteristics of the device which is required to access the service "device fingerprinting" (Khrais, 2015). But, if any of these is compromised, the whole security system would be compromised.

The next section aims at discussing the technologies incorporated by the banks for online security which is followed by the emerging security techniques contemporaneous with the attacks.

SECURITY TECHNIQUES CURRENTLY BEING ADOPTED BY THE BANKS:

Several security layers, consisting of diverse parallel solutions and mechanisms which aim at protecting the banking application and the user's data, providing confidentiality, authentication and authorization.

1. **CAPTCHA (Hasan, 2016):** Completely Automated Public Turing test to state Computers and Humans separately, is a technique employed in some banking systems whose aim is to render bots by generating and rating tests that humans can clear but existing computer programs cannot. Several CAPTCHAs have been developed in recent times. Some are created on Optical Character Recognition (OCR) such as a text CAPTCHA, whereas others are created on Non-Optical Character Recognition (Non-OCR) which requires multimedia, such as voice and video. Some types of CAPTCHAs have been cracked by new bot programs. For example, a text CAPTCHA can be wrecked by using the appliance of segmentation letters. Even though this mechanism proposes fine security and confines automatic cataloguing to web services, some CAPTCHAs have several flaws which allow hackers to penetrate the CAPTCHA mechanism.
2. **Two Factor Authentication:** For any online banking, the main access control mechanism through Internet has been principally user name and password (M, 2017). This simple, single factor authentication has become insufficient in the face of increased cyber fraud activities in current years. The alternate mechanism, which is reasonably more secure and extensively adopted, is two-factor authentication. It requires the users to present two unlike evidence to establish their identity. Two-factor authentication is generally referred to as "something a user has and something a user

knows”(Kruegel & Kirda, 2005). Here, “something a user has” usually involves hardware or software that provides the bank users with an electronically generated passcode or digital certificate. Each bank user has a unique passcode or digital certificate (Sampangi & Hawkey, 2016). Then, the next factor, “something a user knows,” generally means a private password. Clients should use both factors to give them access to critical resources. Two-factor authentication systems are more secure because it is not easy for hackers to get both the factors.

3. Digital Certificates

- a. SSL (Secure Socket Layer) is the foundation of the Internet protection (what-is-ssl.html, n.d.). It secures website and handles the confidential and sensitive information of the users like credentials by providing critical security, privacy and data integrity. It is important to send the information across the network in an encrypted form, such that only the recipient who is supposed to access can comprehend it, maintaining its integrity. The information is unidentifiable to everyone when an SSL certificate is added to the website and it ensures the security of the important information of the users from phishers, hackers and identity thieves. SSL certificates provide authentication to ensure that the data is being sent to the right server. SSL certificates like EV SSL Certificates, asks for more verification and validation than the common SSL certificates. Extensive checking like verification of legally registered organisations, their address and phone number, ensuring if they have a right to use the domain, authorizing the person ordering the certificate and checking that the organisation is not on any blacklists of the government. Visual cues, like lock icon or a green bar make sure that users of the website feel secured. When a SSL-secured website is accessed by a browser, then web server and browser tries to form an SSL connection using a method called an “SSL Handshake”. User cannot see a Handshaking process as it occurs instantaneously. When a browser accesses a website that is safeguarded by SSL, the browser and the web server institute an SSL connection by means of “SSL Handshake”. ([digicert.com/ssl/n.d.](http://digicert.com/ssl/n.d)) SSL Handshake occurs instantly and is imperceptible to the user. Basically, three keys associate the SSL connection: the public, private, and session keys. Encryption with the public key can only be decrypted with the private key, and vice versa. After the secure connection is created, the session key is used to translate all transmitted data.
- b. The latest version of SSL (3.0) which is known as Transport Layer Security (TLS). Algorithms like 1.0. RSA, AES & SHA1 are used for encryption & decryption of the text. TLS has sturdier message authentication, key-material generation and other encryption algorithms. For instance, TLS provisions pre-shared keys, protected remote passwords, elliptical-curve keys and Kerberos whereas SSL does not. TLS and SSL are not interoperable, but TLS proposes backward compatibility for older devices that are still using SSL. The TLS protocol specification explains two layers. The TLS record protocol provides connection security, and the TLS handshake protocol allows the client and server to validate each other and to exchange security keys before any data is transmitted.

EMERGING SECURITY TECHNIQUES RECOMMENDED FOR BANKS:

1. **Certificate Transparency:** Google's Certificate Transparency project repairs several operational defects in the SSL certificate system, which is the key cryptographic system that triggers all HTTPS connections. These flaws deteriorate the reliability and efficiency of encrypted Internet connections and can compromise acute TLS/SSL mechanisms, including domain confirmation, end-to-end encryption, and the chains of trust established by certificate authorities. If left unrestricted, these faults can enable a wide range of security attacks, like website spoofing, server impersonation, and man-in-the-middle attacks. Certificate Transparency aids in eradicating these errors by providing an open framework for checking and auditing SSL certificates in nearly real time (Laurie, Langley, & Kasper). In detail, Certificate Transparency senses SSL certificates that have been erroneously distributed by a certificate authority or malevolently acquired from an otherwise flawless certificate authority. It also makes it possible to recognize certificate authorities that have gone scoundrel and are maliciously handing out certificates.
2. HTTP Security Response Headers
 - a. HTTP Strict Transport Security (HSTS) is a web safekeeping policy contrivance that aids to protect websites against protocol downgrade outbreaks and cookie hijacking. It allows web servers to assert that web browsers (or other conforming user agents) should interrelate with it using only protected HTTPS links, and never via the apprehensive HTTP protocol. The HSTS Policy is linked by the server to the user agent via a HTTPS response header field termed "Strict-Transport-Security" (en-US/docs/Web/HTTP/Headers/Strict-Transport-Security, n.d.). HSTS Policy agrees on a period of time during which the operator agent should only contact the server securely (Hodges, Jackson, & Barth, 2018). As the HSTS HTTP Header is only renowned when directed over a HTTPS connection, websites can still allow users to network with the website using HTTP, to allow compatibility with non-HTTPS user agents.
 - b. HTTP Public Key Pinning (HPKP) is a safekeeping policy that tells a web client to associate a detailed cryptographic public key with a certain web server to cut the jeopardy of MITM attacks with bogus certificates (Evans, Palmer, & Sleevi, 2015). Web clients such as browsers trust a lot of these CAs, which can all form certificates for arbitrary domain names. If an invader is able to compromise a single CA, they can execute MITM attacks on numerous TLS connections. HPKP can evade this risk for the HTTPS protocol by telling the client which public key fits in to a certain web server. HPKP is a Trust on First Use (TOFU) procedure. (en-US/docs/Web/HTTP/Public_Key_Pinning, n.d.) The first time a web server interacts with a client via a distinct HTTP header which public keys belong to it, the client keeps this information for a given period of time. When the client visits the server again, it believes at least one certificate in the certificate chain to hold a public key whose fingerprint is already known via HPKP. If the server distributes an unknown public key, the client should present a cautionary to the user.
3. Analysis Tools and Big Data (Bhasin, 2016)

The industry is progressively responsive of the need for programmed analysis tools that recognize, and account fraud attempts timely. Solution providers are providing instantaneous transaction screening, third-party screening as well as compliance resolutions.

Data Visualization Tools: These are being used to propose a visual demonstration of multifaceted data configurations and outliers to decipher multidimensional data into evocative pictures or graphics.

Behavioural Analytics: This is helping businesses recognize enemies masked as customers. The data analytics applied by the institutions to understand customer behaviour, preferences, etc. are also serving in the detection of fraudulent activity either in real-time or post mortem. The industry is progressively responsive of the need for programmed analysis tools that recognize, and account fraud attempts timely. Solution providers are providing immediate transaction screening, third-party screening as well as compliance resolutions.

- a. The organization inputs every consumer's transaction history and procedures a comprehensive side-view based on their digital banking behaviour where and when they typically transact, their systematic variety of counter parties, the methods they typically access the bank's systems and the standard size of transactions (NG_Digital_banking_fraud.pdf). This technique is functional both to individual customers and to organizational financial accounts that have multiple authorized users. The profile that the system generates becomes part of the pattern against which every future digital banking transaction is associated to assess whether it matches the customer's well-known patterns of behaviour. This behavioural figures is amplified by a wide range of contextual information variables such as the customer's geolocation, time of day, week and month, the device, web browser and type of webpage that is being observed, the kind of account involved (individual or institutional, for example), the domestic or international destination of any payments, whether the payee is first-hand or previously known, and so on. When distinct transactions are assessed against the risk model, it calculates the probability that the transaction is deceitful based on the explicit conditions in which it takes place and the level to which it deviates from the familiar pattern of behaviour related with that account. Significantly, where some anti-fraud systems analyse transactions by size alone, flagging everything above a certain worth, advanced systems appeal on a wider range of contextual information to emphasis the search.
- b. Most anti-fraud systems that employ advanced analytics, incorporating comprehensive user profiles, cannot function in real time and risk failing to sense fraudulent activity quickly enough to avert losses. The efficacy of technology-based anti-fraud systems depends crucially on their capacity to operate in real time, so that suspicious activity can be flagged instantly and transactions blocked. However, the most advanced anti-fraud systems employ Big Data technology, permitting them to apply the advanced analytical techniques to vast volumes of transactions in real time.
- c. **SIEM** (security information and event management) software is installed in order to tackle today's sophisticated cyberattacks. Organizations need to have access to analytics-driven SIEMs that utilises a big data platform that is augmented for machine data with innovative analytics, threat exposure, monitoring tools, incident response tools and threat intelligence.
4. **Deep Learning (Bhasin, 2016; Digital Banking Fraud: Best Practice for Technology-Based Prevention):** It is a technique that teaches computers to do what naturally comes to humans i.e learn by example. The deep learning works on complex algorithms which are based on building hierarchy of abstraction in which each layer is created by the knowledge gained by previous layer. Each algorithm in the hierarchy applies a nonlinear transformation on its input and uses what the knowledge to create a statistical model as output. Iterations will continue until the output reaches an acceptable level of accuracy. In a deep learning process, the data scientist identifies the relevant data sets and prepares them for analysis, chooses and then trains the algorithm on large amount of labelled data and then finally tests the model's performance against unlabelled data.

Internet payment companies providing replacements to traditional money transmission methods are using deep learning, this new method to machine learning and artificial intelligence that is good at recognizing complex patterns and features of cybercrime and online fraud. It can be used to detect suspicious users and thus can help in preventing the potential frauds.

The above technologies should be employed by every bank to keep in pace with the growing technologies behind the attacks. But the security of banking systems is also the responsibility of the users along with the banks and therefore requires knowledge of the topic on the part of the individuals. Having studied about the security measures employed at the bank level, we will discuss the measures that should be taken by the users for the secure handling of online transactions in the following section, as complete awareness at the client's part is also required.

MEASURES THAT SHOULD BE TAKEN WHILE DEALING WITH ONLINE TRANSACTIONS:

1. **Check the Activity of Your Online Account Regularly:** This may be the single most effective strategy one can employ to secure the account and keep a check on any unauthorized access.
2. **Create a Strong and Uncrackable Password:** Passwords should always be a combination of uppercase, lowercase alphabets, numbers and special characters. They should not be kept on basic personal information which can be easily guessed and cracked. Also they should be changed regularly.
3. The passwords, PIN, and other account details should not be shared with anyone and should be memorized.
4. **Never Click on Suspicious Links or Links Embedded in Mails:** It is easy for scammers to set up convincing emails. The users should never click on links contained in mails received from banks. The right way is to type in the bank's website in your browser and navigate from there.
5. **The Users Should Never Give any Account Information Over the Phone or on Mail:** Banks never ask for this information and the calls and mails could be from fraudsters.
6. **One Should Always use Anti-Virus Protection Software, Firewalls and Spyware Blockers and Keep the Softwares Updated:** by keeping these basic computer protections up to date, one can greatly reduce the vulnerabilities of being attacked by the hackers.
7. **Online Banking Should Only be Used on Secure Wi-Fi Networks:** Banking on public networks is not at all recommendable. The low level of security on such networks can be a prime target for attacks.
8. **Always Check for Secure Connections:** While browsing a bank's website and making online transactions, one should be careful of secure connections, if the web address starts from https, it is considered safe.
9. **Always Use Official Banking Applications:** These legitimate apps are tested to ensure the data is secure.
10. **Always Log Out When the Session is Complete:** This mitigates the chances of leaking the information, especially when you are in a public space where not logging off from online account can lead someone else to have access to the sensitive information.

CONCLUSION

4

Cyber-fraud has become a worldwide illicit industry comprising skilled and trained criminals with extreme technological knowledge and access to very sophisticated tools along with the awareness of how financial system works. The level of complexity of frauds is increasing day by day with involvement of more and more people due to which advancement of prevention technologies and security also needs to be evolved. It was discussed how the implementation of SSL certificates, HTTP Security Response Header and Certificate Transparency are most advanced methods to make the E-banking websites secure. The most progressive anti-fraud systems on the market today are using Big Data technology to apply innovative analytical models in real time, giving banks the ability to recognize and block apprehensive activity as it occurs. Machine learning has also become a crucial implement in advanced anti-fraud systems and a prominent growth in its role is going to be witnessed in the upcoming times. New generations of risk modelling, using machine-learning systems that have been developed to spot fraudulent transactions amid vast volumes of banking data, are starting to replace the statistical, probability-based approach that has been used up to now.

Many of the frauds we see today are also happening at user end where the hackers trick the users into giving their personal information and sensitive data which is used to an advantage of the attacker for committing fraud. So, the banks need to employ online banking systems whose security is as user independent as possible. Security measures at both the levels are mandatory for keeping this issue of frauds in check. Looking at this perspective, computer experts are working on creating anti-fraud systems that are more sensitive to the complex patterns of fraud and collusion that are a feature of professionally executed Cyber-frauds. Sensitive systems will allow banks to create an improved equilibrium between detecting frauds and allowing customers to carry out their transactions unhindered.

Improvement in technology and development of innovative techniques based on machine learning can give banks potential access to sophisticated systems that are more effective and more efficient, thus mitigating the chances of frauds.

REFERENCES

Algerian National Extradited from Thailand to Face Federal Cyber Crime Charges in Atlanta for Spy-Eye Virus. (2013). Retrieved from The FBI, Federal Bureau of Investigation: <https://archives.fbi.gov/archives/atlanta/press-releases/2013/algerian-national-extradited-from-thailand-to-face-federal-cyber-crime-charges-in-atlanta-for-spyeye-virus>

All about digital banking fraud prevention. (n.d.). Retrieved from Net Gaurdians: <https://www.netguardians.ch/digital-banking-fraud/>

Bhasin, D. M. (2016, Feb.). The fight against bank frauds: Current scenario and future challenges. *Ciência e Técnica Vitivinícola*.

digicert.com/ssl/. (n.d.). Retrieved from [www.digicert.com](https://www.digicert.com/ssl/): <https://www.digicert.com/ssl/>

en-US/docs/Web/HTTP/Headers/Strict-Transport-Security. (n.d.). Retrieved from <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

en-US/docs/Web/HTTP/Public_Key_Pinning. (n.d.). Retrieved from https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning

Evans, C., Palmer, C., & Sleevi, R. (2015, April). *Public Key Pinning Extension for HTTP*. IETF. doi:10.17487/RFC7469

Fake-banking-sites-wrongly-issued-with-authentication-certificates.html. (n.d.). Retrieved from <https://www.telegraph.co.uk/technology/internet-security/11928690/Fake-banking-sites-wrongly-issued-with-authentication-certificates.html>

Fraud, D. B. (n.d.). *Best Practice for Technology-Based Prevention*. Retrieved from <https://www.net-guardians.ch/>

Hasan, W. K. (2016, June). A survey of current research on Captcha. *International Journal of Computer Science & Engineering Survey*, 7(3), 21.

HatuqaD. (n.d.). Retrieved from <https://www.aljazeera.com/news/2015/09/algerian-hacker-hero-hoodlum-150921083914167.html>

Hodges, J., Jackson, C., & Barth, A. (2018, January 31). *HSTS Policy*. HTTP Strict Transport Security (HSTS). IETF. doi:10.17487/RFC6797

Holtz, M., David, B., Deus, F. E., de Sousa, R. T., Jr., & Laerte, P. (2011). *A formal classification of Internet Banking Attacks and vulnerabilities*. Academic Press.

Hossein Hassani, X. H. (2018, July 20). *Digitalisation and Big Data Mining in Banking*. Academic Press.

how-ct-works. (n.d.). Retrieved from <http://www.certificate-transparency.org/how-ct-works>

Hutchins, E. M., Clopp, M. J., & Amin, P. R. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Lockheed Martin Corporation.

JainM. (2018, May 30). Retrieved from https://www.business-standard.com/article/economy-policy/at-18-indian-customers-biggest-victims-of-banking-fraud-fis-study-118052900467_1.html

Khrais, L. T. (2015). Highlighting the Vulnerabilities of Online Banking System. *Journal of Internet Banking and Commerce*, 20(3). doi:10.4172/1204-5357.1000120

Kim, Y., Kim, I., & Park, N. (2014). *Analysis of Cyber Attacks and Security Intelligence* (Vol. 274). Mobile, AL: Ubiquitous, and Intelligent Computing. doi:10.1007/978-3-642-40675-1_73

King, S. T., & Chen, P. M. (2006). implementing malware with virtual machines. *IEEE Symposium on Security and Privacy (S&P'06)*.

Kiyavash, N., Koushanfar, F., Coleman, T. P., & Rodrigues, M. (2013). A Timing Channel Spyware for the CSMA/CA Protocol. *IEEE Transactions on Information Forensics and Security*.

Kruegel, C., & Kirda, E. (2005). Protecting users against phishing attacks. *The Computer Journal*.

Laurie, B., Langley, A., & Kasper, E. (n.d.). *Certificate Transparency*. IETF. doi:10.17487/RFC6962

Lee, N. (2013). Cyber Warfare: Weapon of Mass Disruption. In *Counterterrorism and Cybersecurity* (2nd ed.). New York, NY: Springer New York.

M, S. S. (2017). *Authentication tokens facilitate secure transactions in the banking Sector*. Academic Press.

NG_Digital_banking_fraud.pdf. (n.d.). Retrieved from https://static1.squarespace.com/static/551aff08e4b037a3bf1ac8c0/t/59dc80663e00bed1b42b612a/1507623017887/NG_Digital_banking_fraud.pdf

Saeed, I. A., Campus, J. B., Selamat, M. A., Ali, M., & Abuagoub, M. A. (2013). A Survey on Malware and Malware Detection Systems. *International Journal of Computers and Applications*.

safe-browsing-protecting-web-users-for.html. (n.d.). Retrieved from <https://security.googleblog.com/2012/06/safe-browsing-protecting-web-users-for.html>

Salomon, D. (2010). *Trojan Horse. s Elements of Computer Security*. London: Springer-Verlag London Limited. doi:10.1007/978-0-85729-006-9

Sampangi, R., & Hawkey, K. (2016). Who Are You? It Depends (On What You Ask Me!): Context-Dependent Dynamic User Authentication. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association.

Security engineering: a guide to building dependable distributed systems. (2008). In R. J. Anderson (Ed.), *Security engineering: a guide to building dependable distributed systems*. Indianapolis, IN: Wiley.

Subrahmanian, V. S., Ovelgonne, M., Dumitras, T., & Prakash, B. A. (2013). *The Global Cyber-Vulnerability Report, no. November 2013*. Cham: Springer International Publishing.

Vilà, J. A. (2015). Identifying and combating cyber-threats in the field of online banking. Barcelona: Academic Press.

what-is-ssl.html. (n.d.). Retrieved from <https://www.sslshopper.com/what-is-ssl.html>

Zolkipli, M. F., & Jantan, A. (2010). Malware Behavior Analysis: Learning and Understanding Current Malware Threats. *2010 Second International Conference on Network Applications, Protocols and Services*. 10.1109/NETAPPS.2010.46

Zolkipli, M. F., & Jantan, A. (2011). An approach for malware behavior identification and classification. *Computer Research and Development (ICCRD), 2011 3rd International Conference*.

KEY TERMS AND DEFINITIONS

CAPTCHA: Completely automated public Turing test to state computers and humans separately is a technique implemented in some banking systems whose aim is to render bots by creating and rating tests that humans can clear but existing computer programs cannot.

Certificate Transparency: Google's certificate transparency project repairs several structural defects in the SSL certificate system, which is the key cryptographic system that triggers all HTTPS connections.

HPKP: It is a safekeeping policy that tells a web client to associate a detailed cryptographic public key with a certain web server to cut the jeopardy of MITM attacks with bogus certificate.

HSTS: It is a web safekeeping policy contrivance that aids to protect websites against protocol downgrade outbreaks and cookie hijacking.

HTTP: It is a web safekeeping policy contrivance that aids to protect websites against protocol downgrade outbreaks and cookie hijacking.

Malware: Malware, or malicious software, is any program or file that is detrimental to a computer operator. Malware comprises computer viruses, worms, Trojan horses and spyware.

Phishing: It is a deceiving technique which involves social engineering (that refers to psychological manipulation of people into performing actions or divulging confidential information) and technical subterfuge.

SIEM: Security information and event management.

SSL: It is the foundation of the Internet protection. It secures website and handles the confidential and sensitive information of the users like credentials by providing critical security, privacy and data integrity.

TLS: The upgraded version of SSLv3.

Tackle the Smart Contract Vulnerabilities

4

Parthasarathi R.

Delhi University, India

Puneet Kaushal

Lucideus Technologies, India

INTRODUCTION

The advent of Blockchain technology led the way towards the development of an electronic contract called Smart Contract. Technically, a smart contract is a computer program that is deployed and running on blockchain they are immutable, public and decentralized (Szabo 1997). The decentralized model of immutable contracts denotes that the execution and output of a contract are validated by each participant in the system so that no single party/participant is in control of the money. That is, no one could force the execution of the contract to release the funds, as this would be made invalid by the other participants in the system. Tampering with smart contracts becomes almost impractical.

BACKGROUND

This section briefly features the nature and the need for smart contracts technology along with its basic properties.

What Are Blockchain and the Smart Contract?

A blockchain is a cryptographic database (ledger) maintained by a network of computers, each of which stores a copy of the most up-to-date version. A blockchain protocol is a set of rules that dictate how the computers in the network, called nodes, should verify new transactions and add them to the database.

A smart contract is an electronic form of conventional contract/agreement deployed and running on the blockchain which executes the terms of the contract automatically without any need of trusted third parties (mediator, court, etc) for the effective implementation.

Figure 1 depicts the sample use case of smart contract in the Business (farmer) to customer model.

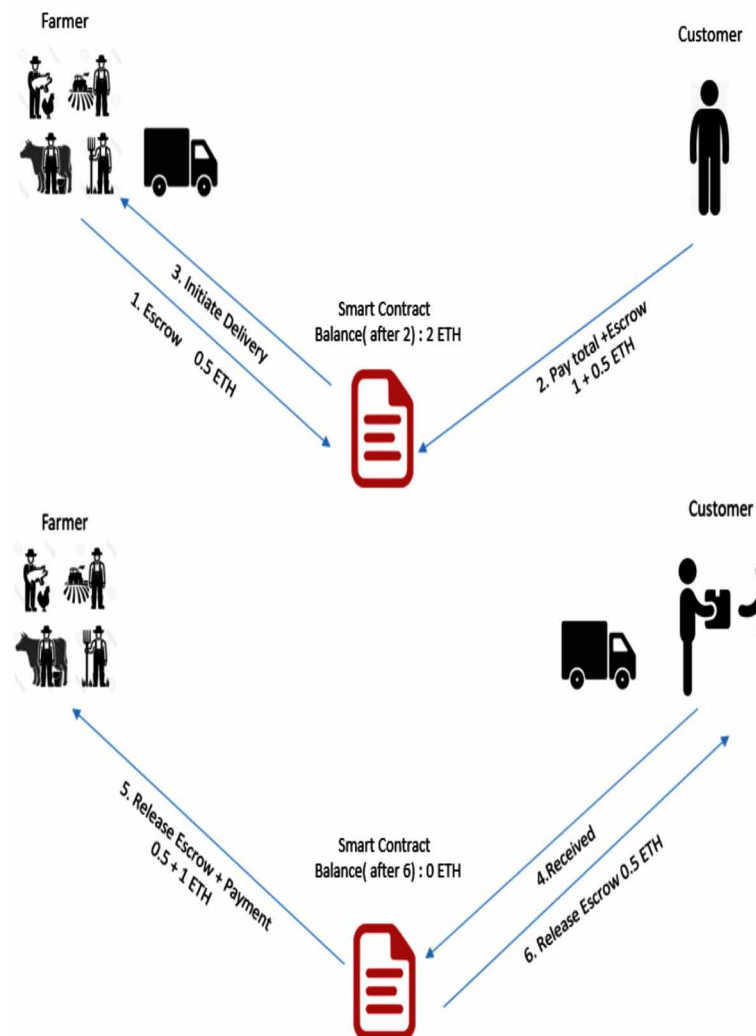
Need for the Smart Contract

Traditional transactions are built on trust and, usually, contracts are considered as a symbol for an existing business deal by the contracting parties. Another major problem with the traditional contracts is that they do not provide enough details about the actual transaction process and as a result. Friction with conflicts between the contracting parties is more frequent (alexafana 2016).

The above mentioned problems are addressed effectively by the development of a smart contract. In general from the viewpoint of information technology smart contract is viewed as an online program, in reality, it is a multidisciplinary concept that also concerns finance/business and contract law, each with

DOI: 10.4018/978-1-5225-9715-5.ch062

Figure 1. Farmer to customer transaction using smart contract



the different perspective (Chapter 9: Building a Secure Future, One blockchain at a time 2018). That is, from the viewpoint of business, a smart contract defines how transactions and payments are executed among different accounts. From the viewpoint of contract law, a contract is an agreement between mutually committed parties (Ustbmde 2018). Because of its interdisciplinary nature, development of smart contract needs collaboration between many experts such as business experts, software and information security engineers, lawyers, and bank managers from different domains (He, et al. 2018).

Properties of Smart Contract

Everything that runs on a blockchain required to be immutable and should have the capability to run through multiple nodes without any compromise on integrity. In order to achieve that, smart contract functionality needs to have three things in common:

Deterministic

A deterministic program is the one that gives the exact output every single time for the particular given input. That is, if the output for $5+1$ is 6 then $5+1$ ALWAYS will have 6 as an output (assuming the same base). But, there are numerous moments a program can act in an un-deterministic manner:

Calling Un-Deterministic System Functions

Un-deterministic data resources: If a program receives the data from the un-deterministic data source during runtime then it becomes un-deterministic.

Dynamic Calls: Dynamic calling occurs when a program calls another program in which the target of the call is decided only during execution.

Terminable

In 1936, Alan Turing, a mathematician, deduced using Cantor's Diagonal Problem, that there is no way to predict whether a given program can finish in a time limit or not, this unknown execution time inability is known as the Halting Problem.

In smart contracts, this is an apparent problem because contracts must have the capability to terminate in the given time limit. There are few corrective actions have taken to ensure that the contract does not enter into an endless loop which will drain the resources. To tackle this terminable problem, below mentioned properties are used by smart contracts

Turing Incompleteness: Since Turing, Incomplete blockchain have only limited functionality, for example, to avoid endless loop jumps and/or loops are not allowed.

Step and Fee Meter: A program can plainly keep track of the number of steps it has taken and terminate when a particular step count has been reached. Another method is the Fee meter, where the contracts are executed with a predefined fee and for every instruction execution requires a particular amount of the fee. When the fee spent exceeds the predefined fee the contract gets terminated automatically.

Timer: the predetermined timer is used, If the contract execution exceeds the specified time limit then contract to get aborted externally (Atzei, Bartoletti and Cimoli, SoK: unraveling Bitcoin smart contracts 2018).

Isolated

In a blockchain, almost anyone can upload a smart contract. Because of this feature, the contracts may contain malicious code. So a non-isolated contract may damage the entire system. Hence, isolation of smart contract in the sandbox is very important to save the entire ecosystem from any negative effects (blockgeeks.com, A Deeper Look at Different Smart Contract Platforms 2018).

While smart contracts promise much to consumers, due to its complex properties, interdisciplinary nature and underdevelopment phase, there is a strong possibility of harming the consumer if proper regulation is not in place.

This paper intended to focus on such common vulnerabilities and proposed effective security measures to tackle the potential risks along with the future development area to avoid security risks.

VARIOUS COMMON VULNERABILITIES

This section briefly explains the most common vulnerabilities, which result in huge financial losses in the past few years.

Generally, smart contracts represent a new blockchain attack vector that hackers can compromise by applying other methods that are typical for compromising blockchain technology, including DDoS, eclipse, and various low-level attacks.

Basing on a recent study performed on nearly 1 million Ethereum smart contracts, 34,200 of them were discovered as vulnerable. That surprising number was attained by analyzing trace vulnerabilities of smart contracts including:

- Finding contracts that lock funds indefinitely-Greedy contracts
- Contracts that lack funds carelessly of arbitrary users-Prodical contracts
- Contracts that can be killed by anyone-Suicidal contracts (Han, et al. 2018).

Along with the general logical complexity and novelty associated with programming smart contracts, their immutable nature makes vulnerabilities potentially much more damaging (Curran 2018).

The main blockchain security issues associated with smart contracts relate to possible bugs in source code, a network's virtual machine, the runtime environment for smart contracts, and the blockchain itself. Let's have a closer look at each of these attack vectors.

For easy understanding, the following solidity vulnerable smart contract code has been used throughout the paper as a reference to explain the numerous vulnerabilities.

```
pragma solidity ^0.4.18;
contract Sample_wallet{
// owner variable specify the owner address
// balances variable is used to maintain the users balance
address public owner;
mapping(address=>uint256) balances;

// Constructor for assigning the owner address
function Samplewallet() public {
owner=msg.sender;
}
//Modifier used to check a condition before executing the function
modifier owner_only {
require(msg.sender==owner);
_;
}

// Kill function uses selfdestruct function to kill the contract and send re-
maining ether to specified address
function kill() owner_only public {
selfdestruct(owner);
}
```

```
// Deposit function allows the user to deposit ether to his account
function deposit() public payable {
    balances[msg.sender] += msg.value;

}

// Transfer function is used to transfer ether from the user account to the
specified "to" address
function transfer(address to, uint _token) public {

    require(balances[msg.sender] > 0);
    require(to.call.value(_token)());
    balances[msg.sender] = balances[msg.sender] - _token;
}
}
```

The above vulnerable contract is the simple wallet contract which takes the token (ethereum cryptocurrency) from the user via deposit() function, and allows him to transfer his token to any specified account of his choice by calling transfer() function. It also allows the contract owner to kill the contract at any time by calling kill() function.

Choosing the Platform

There are many smart contract platforms available with various properties which make them unique. There is no “one-size-fits-all” yet. Hence, users have to choose the platform that best suits the functionality requirement of their Dapp(Distributed Application).

Since it's a new technology, all the platforms are still evolving, every platform has its own kind of vulnerabilities. The wrong choice could lead to irreversible stability, scalability, security issues which in turn results in a huge financial loss. So choosing the best fitting platform for the application itself is a challenging task as now.

In Virtual Machines

Each blockchain platform has its own virtual machine/docker to execute the smart contract. That is, each virtual machine/docker has its own set of vulnerabilities, few are universal, few are unique to the virtual machine.

Let's take an example of the most commonly used Ethereum Virtual Machine (EVM) and its vulnerabilities.

EVM is a distributed stack-based computer runtime environment used for Ethereum's smart contracts where all smart contracts of Ethereum-based bloodstains are executed. The most common vulnerabilities of the EVM are as follows:

Short-Address Attack: EVM can accept incorrectly padded arguments, hackers can exploit this vulnerability by sending specifically crafted addresses to potential victims. For instance, during a successful attack on the Coindash ICO in 2017, a modification to the CoindashEthereum address made victims to send their Ether to the hacker’s address (Bryk 2018).

[illegible]

Vulnerabilities in smart contract source code constitute a threat to parties that sign the contract. Because bugs in source code are impossible to fix due to its immutable nature. This risk makes the cybercriminals to discover and exploit code vulnerabilities to steal cryptocurrency or create a new fork, as happened with the DAO attack (DuPont 2017).

The following is a list of few known attacks which can be avoided. The comprehensive list of attacks is provided in the ADDITIONAL READING (Manning 2018) section for reference.

The Overflow Error

An overflow arises when a number gets incremented beyond its maximum value.

Let's see the snippets from solidity:

```
uint8 Value = 255;
```

```
Value++;
```

In Solidity unsigned integer of 8 bit can take value from 0 to 255. So incrementing Value by 1 would lead to an overflow situation which set the Value to 0. Developers must be aware before declaring the variables.

The Underflow Error

The Underflow error, on the other hand, work in the exact opposite direction. Let have a look at another example, uint8 can take values only between 0 and 255.

Consider the following snippets

```
uint8 Value = 0;
```

```
Value--;
```

Decrementing the Value by 1 lead to underflow situation which will set the Value to 255.

The underflow error is more often than the overflow error because it will be somewhat impossible for someone to get the required number of tokens to cause an overflow(blockgeeks.com, Understanding Overflow and Underflow Attacks on Smart Contracts 2018).

Consider this scenario in the above mentioned vulnerable contract. The malicious user is having a balance of 5 tokens, that is, balances[msg.sender]=5. If he calls the transfer() function with _token value as 6.

The code line in the transfer() function balances[msg.sender]=balances[msg.sender]-_token will get executed as balances[msg.sender]=5-6. This subtraction leads to underflow, where the user balances[msg.sender] will be credited with a positive number (2^{256}).

Race Conditions

Race Conditions are a general system's behavior where events do not occur in the planned order. Race Conditions may possibly arise in Smart Contracts, from calling external contracts that take over control flow.

Reentrancy is a kind of Race Conditions, in which some function is called repeatedly before the first function invocation is completed. Scrutinization of external calls, that is, to block concurrent calls in certain functions would be the key solution.

In the above-mentioned vulnerable contract if the user calls the transfer() function, first it checks whether the balances[msg.sender] is greater than zero or not. If yes, then it sends the specified token to the specified "to" address and then deduct the token value from the user.

Say the above contract is in a Sample_wallet.sol file and the malicious user create a Hack.sol file with a Hack contract to exploit the external call.

Tackle the Smart Contract Vulnerabilities

```
contract Hack {
Sample_wallet s;
uint public count;
uint etherValue=5;
function Attacker(address vulnerable) {
s = Sample_wallet(vulnerable);
}

function attack(address _to) {
s.transfer(_to,etherValue);
}

function () payable {
count++;
if (count < 10) {
s.transfer(to,etherValue);
}
}
}
```

In Hack.sol, two primary functions are defined. The first is attack() function that calls the transfer() function of Sample_wallet contract. Now, Sample_wallet contract's transfer() function executes the call() function to send 5 tokens to Hack.sol, that in turn triggers the second function, function() payable{ } of Hack.sol which will call the transfer() function again for 5 tokens. The key point to note here is, the initial transfer() function's call() function is not yet completed, so user balance is still the same irrespective of 5 tokens transferred. So calling transfer() function in the loop will transfer 5 tokens every time without deducting the user balance.

Transaction-Ordering Dependence (TOD)/Front Running is another kind of race condition, which allows one user to benefit from a manipulated transaction order at the cost of another user while the transaction being located in a mempool for a short time.

Timestamp Dependence is one of the conditions that allow Front Running, scrutinization of time-stamp usage in a contract is necessary, especially in cases where transaction time is financially important - such as in a betting contract. Because beware that miners can manipulate the timestamp of the block (blockgeeks.com, How to Audit a Smart Contract 2018).

Programmer/Human Error

Smart contracts development requires a different mentality than developing traditional software. It's more like building a monument that you want to last and remain beautiful for a long time than like building a complex mechanism. Even a minimal bug may lead to irreversible damage.

Developer failures are mostly due to

- Misunderstood the objective
- Making a mistake when implementing that objective

Many of these typical errors may be results in huge sums of locked up funds like with Ethereum's recursive send exploit in the DAO incident or with the Parity wallet (Curran 2018).

In our example, function `SampleWallet()` is deemed to be the constructor, but our contract name is `Sample_Wallet`. So solidity will consider it as a normal function which can be called by anyone. If attacker calls this function he will be the owner of the contract which authorizes the attacker to call `kill()` function to kill the contract and send the entire contract balance to attacker's address.

BEST PRACTICES FOR IMPLEMENTATION

This section covers solutions and best practices to tackle the above-mentioned vulnerabilities.

Platform Selection

It's difficult to compare all the platforms because each platform is meant for a specific purpose, so, it just depends on your needs. It's best to consider the maturity of each platform as that's a good indicator (Smooke 2018). The followings are some indicators which can be considered while choosing the platform

Supports Millions of Users: A platform has to be scalable enough for millions of users to use it. This is especially true for DAPPs that are looking for major acceptance.

Free Usage: The platform should enable users to use it for free for the development purpose. That is, the user should not ask to be paid for the platform to gain the benefits of a Dapp.

Easily Upgradable: The platform should have the freedom to upgrade the Dapp whenever the developer wants. Also, if some bug does affect the Dapp, the devs should be able to fix the Dapp without affecting the platform.

Low Latency: Even with the lowest possible latency Dapp have to run as smoothly as possible.

Parallel Performance: In order to distribute the workload and save up time the platform should allow their Dapps to be processed parallel.

Sequential Performance: Multiple transactions cannot be executed in parallel it has to be done one at a time to avoid errors like double spends.

Smart Contract Auditing

An audit is a keen searching for a smart contract code for vulnerabilities, exploitative features, and inefficiencies to provide security against malicious actors and mistake. Audits are crucial to the progression of blockchain implementation and adoption. The new pair of skilled eyes required to view the code through the lens of an auditor is extremely important to secure against cryptocurrency loss, and/or data loss on behalf of the people that cannot. Auditors have to be even more cautious than project developers.

The smart contract audit can be either automatic or manual tests. Mostly automatic audit finds commonly encountered security vulnerabilities whereas manual test outlines efficient, logical, and optimization improvements. A smart contract audit is almost the same as a conventional code audit, it aims at finding security vulnerabilities before the deployment of code. The above-mentioned vulnerabilities like Over/Underflows, Reentrancy, and Front Running are most likely to be discovered using smart contract (Mishunin 2018) auditing.

Auditing Tools As Supplements

There are many software tools available on the market to aid in the auditing practice. Example, for detecting uint overflows and underflows a tool called Mythril can be used. Another tool is called Etherscrape, used to find reentrancy bugs when `send()` is being used. To bring together companies and freelance auditors when tools aren't enough, a decentralized auditing platform called Bountyone can be utilized. Note that, these tools can be employed as an additional security check, but it should not substitute the formal auditing process.

Formal Verification

Even though smart contract auditing provides a very fine layer of vulnerability detection, mathematical analysis, known as formal verification, helps to reduce instances of vulnerabilities further. Formal methods are the kind of mathematical technique used for the specification, development, and verification of both software and hardware systems. The process of accepting or rejecting the appropriateness of the proposed algorithms using a formal method is known as formal verification (Curran 2018).

A formal specification is used as the accurate output or result that a smart contract is expecting for, which a computer can check. After the contract compiled into the bytecode, the formal verification proves that the compiled bytecode implements the specification. However, manually performing formal verifications is a complicated process and at times comes with its own mistakes. And also verifying formal proof results can come with its variations.

Developer's Sharpness

Since blockchain's smart contract handles a huge sum of money, developers need to be very keen and do some sort of basic testing/verification from his side too. The first is a syntax topological analysis of the smart contract invocation relationship, to help developers to understand their code structure clearly; the second is a logical risk (which may lead to vulnerabilities) detection and location, and label results on the topology diagram.

Smart Contract Weakness Classification Registry

A comprehensive up-to-date list of known smart contract vulnerabilities and anti-patterns with real-life examples is found in the Smart Contract Weakness Classification Registry. Browsing the registry is an excellent way to keep updating with the latest attacks (consensys.github.io, Smart-contract-best-practices 2018). Link to the Smart contract weakness classification registry is given in the ADDITIONAL READINGS (smartcontractsecurity.github.io 2018) section.

FUTURE RELATED WORK

Though the above-mentioned solution helps to mitigate most of the common vulnerabilities, in order to ward off such attacks the auditing process should take an engineering approach, stringent verification with a background of theory and practice, as well as tool application. The standard software engineering framework is the need of the hour. The standardized approach helps the developers to code efficiently.

Blockchain-Oriented Software Engineering is needed to define new directions to permit effective software development. Modeling and verification frameworks, enhanced security, reliability, new professional roles, and specialized metrics are needed to take blockchain applications to the next trustworthy level. At least, the following three main areas are addressed as soon as possible.

- Best practices and development methodology
- Design patterns
- Testing

The aim of Blockchain-Oriented Software Engineering is to define new patterns, quality metrics, ad-hoc methodologies, fault analysis, security strategies and testing approaches capable of supporting a novel and disciplined area of software engineering. Still, need lots of research in the Smart Contracts security field (Destefanis, et al. 2018). Even after decades and the development of engineering approaches in traditional software development, the development of bug-free source code, is still a challenge. Error free code is even a more difficult task for blockchain software development, which started less than a decade ago. Vulnerabilities like the one leading to the Parity attack has clearly stated the need for adoption of the standard and best practices in Blockchain Software Engineering.

Testing the smart contract is challenging even critical because after deployment they become immutable, further testing or upgrading is not allowed. At present, smart contracts are not having a proper testing framework, meaning that every smart contract needs to be tested manually. Because of the criticality of the application and disability to update once deployed nature introduces much more complications to test. Hence, it is desirable to utilize, robust testing techniques. Even though manual testing is likely to form an essential component, but is certainly limited; there is a need for effective automated test generation (and execution) techniques.

CONCLUSION

In real business scenarios, especially ones with a complex business model for smart contracts still have a long way to go. As blockchain technology is still an emerging field, there is no go-to resource for all-encompassing solutions. There is also a need to discover a way to update smart contracts to take into account of evolutions, that is, we need a strategy that can be exploited for debugging purposes, refactoring, the new features, and, in general, for purposes similar to the version in traditional software engineering. In the future, smart contracts will need to be much more robust, not only in function but also in flexibility and security, to satisfy multiple business scenario. Nevertheless, as of now, the smart contract security lies in the hands of every stakeholder.

REFERENCES

- alexhafana. (2016). *Smart-Contract Languages Comparison*. Retrieved from <https://steemit.com/smart/@alexhafana/smart-contract-languages-comparison>
- Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. *6th International Conference on Principles of Security and Trust (POST), European Joint Conferences on Theory and Practice of Software*. 10.1007/978-3-662-54455-6_8
- Atzei, N., Bartoletti, M., & Cimoli, T. (2018). SoK: unraveling Bitcoin smart contracts. *7th International Conference on Principles of Security and Trust (POST), European Joint Conferences on Theory and Practice of Software*.
- blockgeeks.com. (2018a). *A Deeper Look at Different Smart Contract Platforms*. Retrieved from <https://blockgeeks.com/guides/different-smart-contract-platforms>
- blockgeeks.com. (2018b). *How to Audit a Smart Contract*. Retrieved from <https://blockgeeks.com/guides/audit-smart-contract/>
- Bryk, A. (2018). *Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology*. Retrieved from <https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors>
- Building a Secure Future, One blockchain at a time*. (2018). US Senate Joint Economic Committee.
- Curran, B. (2018). *How Formal Verification Can Reduce Bugs & Vulnerabilities in Smart Contracts*. Retrieved from <https://blockonomi.com/formal-verification-smart-contracts/>
- Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., & Hierons, R. (2018). *Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering?* IEEE.
- DuPont, Q. (2017). *Experiments in Algorithmic Governance*. Retrieved from <https://web.archive.org/web/20170730133911/http://iqdupont.com/assets/documents/DUPONT-2017-Preprint-Algorithmic-Governance.pdf>
- github.com. (2018). *Smart-contract-best-practices*. Retrieved from <https://github.com/ConsenSys/smart-contract-best-practices>
- Han, Gupta, Tann, & Ong. (2018). *Towards Safer Smart Contracts: A Sequence Learning Approach to Detecting*. Academic Press.
- He, X., Qin, B., Zhu, Y., Chen, X., & Liu, Y. (2018). *SPESC: A specification language for smart contracts*. IEEE.
- Mishunin, D. (2018). *How to perform a smart contract audit?* Retrieved from <https://medium.com/hashex-blog/how-to-perform-your-first-smart-contract-audit-3d6883f44924>
- Smart-contract-best-practices. (2018). Retrieved from https://consensys.github.io/smart-contract-best-practices/known_attacks/
- Smooke, D. (2018). *Dealing With Reality to Get What You Want*. Retrieved from <https://hk.saowen.com/a/5fe6dc23d5b284f3604f8b7bd805473bedc84e45d02a72fd7da98b6166c986cf>

Szabo, N. (1997). *The Idea of Smart Contracts*. Retrieved from <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>

Ustbmde. (2018). *Smart Contract*. Retrieved from <https://bitbucket.org/ustbmde/smartcontract/wiki/Home>

ADDITIONAL READING

Alex, N. (2018). *Self-Aware Smart Contracts with Legal Relevance*. IEEE.

Zhou, E., Hau, S., Pi, B., & Sun, J. (2018). *Security Assurance for Smart Contract*. IEEE. doi:10.1109/NTMS.2018.8328743

KEY TERMS AND DEFINITIONS

Auditing: The process of conducting an official inspection of a company or its accounts.

Blockchain: A digital ledger in which transactions made in cryptocurrency are recorded chronologically and publicly.

Cryptocurrency: A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

DAO: Is an organization represented by rules encoded as a computer program that is transparent, controlled by shareholders and not influenced by a central government.

Dapps: Decentralized applications (dApps) are applications that run on a P2P network of computers rather than a single computer.

Ethereum: Is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

Smart Contract: Is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other.

The Challenges and Future of E-Wallet

Chiam Chooi Chea

 <https://orcid.org/0000-0002-7403-0320>

Open University Malaysia, Malaysia

INTRODUCTION: BACKGROUND

The term “cashless” is heard on a daily basis these days and it is called digital payment with no cold, hard cash involved. The transactions are made via electronic transfers where it only takes a tap of a smartphone or scan of a QR code to complete the process. E-wallet is an electronic device or an online service that enables electronic transactions. This includes purchasing items online, where banking accounts, bank cards, IDs etc can be linked to the digital wallet. Payments or purchases can be made with just a click away, with those banking and personal information stored in the system. E-wallet is surfing on the e-payment world currently and seems to stay for a long time. A note to consider is that digital wallets are not all about making transactions, but also to authenticate the purchasers’ credentials, such as; e-wallet could verify the age of the buyer to the store while purchasing alcohol or cigarettes. E-wallet proposes easy and safe transaction for purchasers as consumers are not required to fill out particulars when they purchase because the information has already been stored or saved in the e-wallet system. Other than that, due to rising number of snatch theft or crimes worldwide, e-wallet is a cashless transaction, hence the safe feature being embossed in it. On the other hand, e-wallets are made available to consumers without any charges.

The term e-wallet, mobile wallet, electronic wallets, virtual wallets, digital wallets, cashless transactions, mobile payments and similar terms are used interchangeably among consumers and sellers. These terms are mobile applications that enable financial transactions. Although e-wallet concept more pros than cons, it may not seem that many people are using e-wallet technology at the moment. Few years ago, most of the players in the banking industry foresee that e-wallets would take over the usage of cash and credit/debit cards (plastics) by consumers quickly. However, e-wallets haven’t exactly taken off and consumers’ reception and interest do not seem to take off and this shows that the concept of e-wallets still have a long way to go. What can be reasons for this phenomenon? Most of the prominent shops, whether it is online or walk-in are introducing the e-wallet concept for its buyers. The question remains, is this the future way of making payment when purchasing online or walk-in? Is the e-wallet function the same as our physical wallet in our actual wallet? Is there only one e-wallet for all the shops and purchases? At this moment, there are many different e-wallets platforms for different shops and each time the purchaser need to top-up or reload money in the e-wallets, it seems to pose as a hassle more than convenience and it is merely almost impossible to really empty the e-wallet to zero amount. There will be somehow some cents or dollars in these e-wallets. The e-wallet is in the current wave for the younger purchasers due to its “cashless” and “pay anytime” concepts. There are many perspectives that need to be considered before e-wallet makes it mark in the market entirely, such as; older generations reception, problems to eye-sight due to age, the e-wallet platform readiness, law pertaining to e-wallet, safety features of e-wallet, new trend of cyber crime arises, internet accessibility, stability and its speed in the country etc all make e-wallet little tougher on rising on a full scale. Other than that, consumers do

DOI: 10.4018/978-1-5225-9715-5.ch063

not seem to like to go through the hassle to change that provide little differences between plastics and e-wallet. Both are cashless and, plastics are somehow very convenient too, just swap and sign or swap with 6-digit pin number at the counter. E-wallets need to have more benefits or perks than plastics in order to win over these plastics consumers. Currently, credit cards are the most popular mode of payment for consumers in the world followed closely with debit cards. Nevertheless; it is difficult to know the future given the stealth ability of e-wallet tools.

FOCUS OF THE ARTICLE: E-WALLET KEY TAKEAWAYS

CMB Consumer Pulse (2015), highlighted several key takeaways for E-Wallet:

- 2015 is the year when mobile payments take off and rewards and discounts won't be the only motivators—Familiarity and usage have doubled since 2013; with 15% having used a mobile wallet in the past 6 months and an additional 22% likely to adopt in the coming 6 months. Rewards and discounts are compelling to potential users but alternate uses including the ability to use a device as a photo ID or in spend management are also compelling.
- Barriers to mobile wallet adoption are diminishing overall—Security concerns remain the number one barrier to mobile wallet adoption—however just 62% of respondents list security as the number one barrier, down from 73% in 2013. The near ubiquity of online shopping (86% have made a purchase from their desktop or laptop in the past 6 months) may be acclimating consumers to perceived security risks like identity theft.
- Wearable technology, often called “wearables,” is clothing or accessories that incorporate computer and advanced electronic technologies. The designs often incorporate practical functions and features, such as pedometers, heart rate monitors and activity trackers. Wearables set to pave the way for mobile wallet adoption. While many consumers don't yet see the benefit to using their phone at the point of sale, the ability to scan a wearable device, like a smartwatch, at the register may help customers overcome this convenience barrier. Nearly 40% of those highly likely to buy wearables in the coming year want it to come with mobile wallet functionality. And the majority of likely wearable buyers claim that the presence/absence of a mobile wallet has a major impact on their purchase decision

E-WALLET FEATURES

E-wallet is known as digital wallet is an electronic device or an online service that enables electronic transactions. E-wallets companies have been ramping up on their infrastructure with several features to capture the interest of consumers. The following are some of the common features of e-wallet:

- Payments are made immediately- Customers can make cashless transactions without much hassle.
- E-wallet apps are free of charge and can be installed rather easy stored with personal and banking details.
- Able to transfer and link to bank accounts and able to make payments via these accounts and e-wallet app.
- Accumulate points and redeem points for cash vouchers or other benefits such as additional offers and discounts vouchers
- Split bill- Several e-wallets apps allow the customers to split the expenses with the same wallet users. Doing this will generate a payment link with banks accounts
- Chat messenger integration- E wallets has integrated its payment service through chat messenger in order to increase your convenience further

Many technology supporters indeed realise the fact that demonitisation is here to stay and the convenience of e-wallets cannot be possibly ignored, hence consumers should take it upon themselves to use cashless transaction methods such as e-wallets to the fullest. Nevertheless, there are many setbacks for e-wallet and it has reached its fullest potential. E-wallets able customers to send payments for things purchased with just a few taps on the mobile phones or laptops. Customers have to follow several steps to complete the transactions and the payment will be deducted from the customers' e-wallet and the amount will be credited into the merchant's e-wallet account. It is similar to face-to-face transactions except it is all done without any physical cash in play. E-wallets have several advantages over physical cash. Digital money is safer to carry around, especially if you need to make large payments. Other than that, it keeps records of all the purchasers' transactions and its amounts, which enables the purchasers to manage their finances in better manner.

TYPES OF E-WALLETS AND ITS PERKS

There are many mobile wallets options to one can choose from and it all matters on individual preference as well as the perks and benefits they offer to its users. Although, there are users who will remain with their bank's app, but many would try out other mobile wallets which offer better features that banks could not match technologically. Some examples of e-wallets which are supported by most mobile devices:

E-Payments Services

It refers to services provided by e-commerce payment systems in online purchases. Mobile apps created by banks is under this category, however the most popular mobile wallets with e-payments services tend to be developed by tech giants. Google Wallet, Apple Pay, Samsung Pay, PayPal which offer comfort to users due to their solid reputation.

Loyalty and Coupon-Based Wallets

Customers these days are very alert and wary on loyalty benefits, coupons-based mobile wallets. Apps such as Gyft, Key Ring and LevelUp are making its way to the customers' choice list due to its perks and benefits. The Starbucks mobile wallet is a favourite among many of its enthusiasts, and offers app-only promotions. These apps can link and store all of your loyalty card accounts under one account and cus-

tomers are still able to use these loyalty cards to collect reward points or bonuses. It provides convenience to customers as they do not have to carry all the cards around when doing their shopping.

Peer-to-Peer Payment Wallets

Mobile wallets such as SquareCash, Venmo and Circle are categorised under peer-to-peer payments between friends and family. It's designed to provide convenience for paying back the money one owes to his/her acquaintances. It is able to eliminate the awkwardness when asking people who owe one's money to pay back.

Cryptocurrency Wallets

Many cryptocurrencies are still not at their mature stage. Bitcoin is the most mature cryptocurrency to date and Bitcoin wallets work like regular wallets, except that instead of USD, the purchaser sends the Bitcoin-value equivalent at the time of payment instead. The merchant will provide a Bitcoin address (alphanumeric code or QR code) that the purchaser can enter as the destination address. The value of Bitcoin changes often, so you might want to time your purchases.

Hybrid Wallets

A hybrid wallet is a form of mobile wallet that supports both digital currencies and traditional cash currencies in the same platform. Wirex is an example of a FinTech service which. It's like a combination of a banking account with Bitcoin wallets. The purchaser's account can have both cash and digital currencies, hence, it's an interesting product as it provides alternatives and options for purchasers and it can be appealing to as each alternative has its benefits one can benefit.

Remittance Wallets

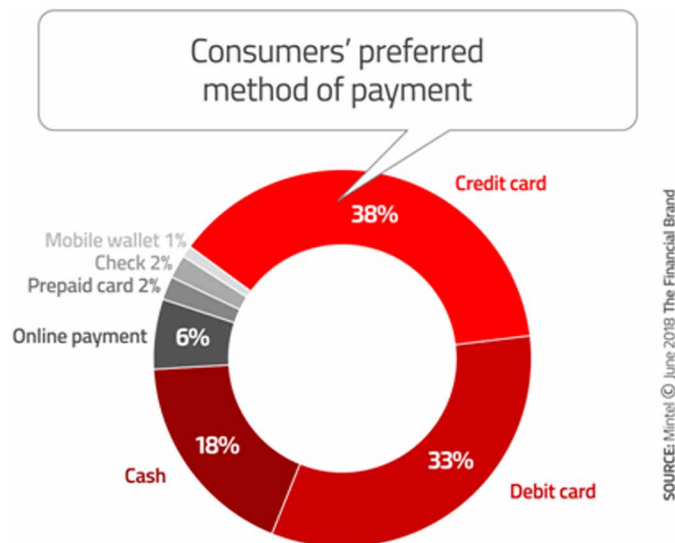
Remittance wallet is similar to peer-to-peer payment wallets, with an additional focus and emphasis on the receiver (who tend to stay in developing or third world countries, where literacy might be an issue) to collect the money. International remittance is a big market. Wallets such as Remitly and Xoom are marketed with this in mind. It is a helpful money-saving tool for people who send money to countries where much of the population are bankless.

Messaging App Wallets

Messaging app wallets are still relatively new. For example WeChat can only be used in some stores in China, and Facebook Messenger just integrated PayPal payments. WeChat, Telegram and Facebook Messenger can all be used to receive money from third party to pay for the products and services.

Figure 1. Consumers' preferred method of payment

Source: Mintel, 2018



CONSUMERS' PREFERRED METHOD OF PAYMENT

In a study by Thrive Analytics (2018), socio economic demographics were the key factors in capturing “new consumers” for e-wallet services. Refer to Figure 1 and Figure 2 for the details on consumers' preferred method of payment as well as consumers who do not want to change their payment methods. Key findings from Mintel (2018), the survey indicated that consumers do carry lesser cash today, especially females, with 50 percent of all consumers carrying less than \$20 on a regular basis. From the survey results, three out of four are under the age of 40 do not carry any cash at all. Other than that, approximately 60 percent of all digital wallet users are male despite carrying more cash than females. Females (18-29 years old) tend to use merchant digital wallet apps more often than males to look for discounts/ coupons, with 72 percent and price shop, 56 percent. Meanwhile, males tend to browse and engage in service related activities such as paying bills and browsing through retailers' product and contact information when they use merchant apps. The most digital wallet usage was done through mobile phones with approximately 60 percent for purchases under \$10; with entails daily products such as groceries, retail items, games and books.

WORLDWIDE MOBILE PAYMENT PLATFORMS IN 2017

The highest number of users in the mobile payment platform is Wechat pay, which is widely and popularly used in China due to the fact that China is rising as a one of the leading countries in the world. This may be due to the fact that, it has since practiced open economy with the introduction of its “one belt one road” concept to the world, besides of being one the most populated countries in the world. China is one of the largest markets in the world and this makes China is a strong spending power due to

Figure 2. Consumers who do not want to change their payment methods

Source: Mintel, 2018

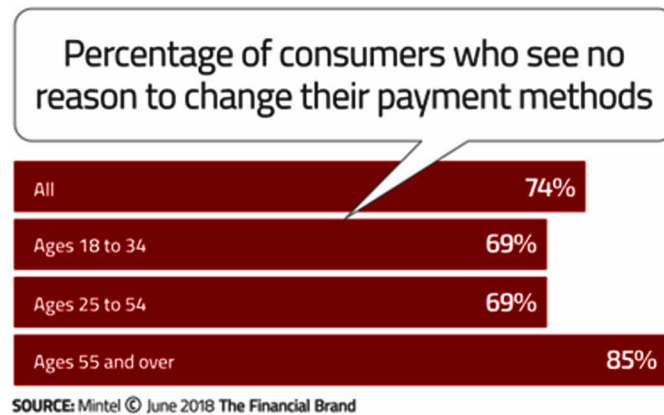
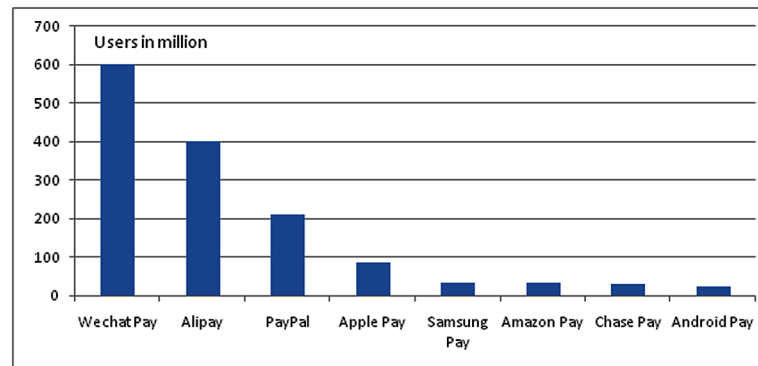


Figure 3. Statistic reports on the number of users of selected mobile payment platforms as of August 2017

Source: The Statistical Portal, 2017



its high number of consumers from the country. Refer to Figure 3 for the statistic reports the number of users of selected mobile payment platforms as of August 2017. According to the findings, 600 million users had been reported to have used WeChat Pay as their mobile payment platform. Alipay was ranked second with 400 million users worldwide.

Challenges of E-Wallets

According to Vulcan Post (2017), there are many challenges and obstacles that e-wallet faced and the expected reception for e-wallet is not as good as expected due to several seen and unforeseen factors:

Setting Up Can Be Hassle

Although the e-wallet concept promises easy and seamless transaction, nevertheless the start-up may not be as easy as one thinks and can pose as a hassle for the users even more if one have never used cashless before and are not sure what to do. There might be a need to give banks a call to enable e-commerce transactions and the fact that some additional efforts are needed can deter users.

Lack of Trust on E-Wallet

According The Financial Brand (2018), consumers may like the idea of a cashless society, but they still have serious reservations about mobile wallets due to many reasons, with security issues topping the chart. Approximately 43% of consumers don't think mobile wallets are secure, and 38% are concerned about losing their device and therefore being unable to make any payments. In the same study, it was found that more than half (55%) of consumers prefer to use credit cards due to safety concerns.

It Is Not Entirely Free

Although a wallet is free for consumers, vendors charge merchants for wallets. Some wallet vendors make arrangements for merchants to pay them a percentage of every successful purchase directed through their wallets. In other cases, digital wallet vendors process the transactions between cardholders and participating merchants and charge merchants a flat fee and that fee are usually transferred to the consumers.

Security Features Issues

Although retailers and merchants tout the best cashless system with its best security protection software and firewalls, there is no guarantee that the system will work smoothly without any flaws. There is a saying "there is never a guarantee with anything that deals with technical issues". Although all are in order, the system can be down or crashed in just a few seconds. No system can guarantee with 100% assurance that data wouldn't be stolen, and money siphoned off. Many were taken aback with technology when there is hack or "taken hostage" in the laptop or personal computer itself. Eg. The ransomware WannaCry that managed to shut down entire companies from operating due to a small flaw in the Windows systems they were running.

Fear of Cyber Attacks

Due to revolution and the rage wave of cashless, hackers are getting bolder and better at cracking the security firewall of these security firewalls and security systems for cashless. Regardless of how well the retailers and owners of these cashless systems tout the best protection of these security software and firewalls, there will be no 100 percent guarantee with 100 assurance that the data will not be stolen or hacked or taken "hostage". One of the cyber attacks that make its way to the headlines lately is a ransomware "WannaCry" that is able to take "hostage" and threatened to shut down entire companies from operating due to a small flaw in the Windows systems they were running.

Not Enough Shops Adopting Cashless, or Implementing It Well

Although the cashless payment terminals are going viral but at times the terminal is not really functioning or the system is down at the store. This poses a real nuisance, and instils disappointment, dissatisfaction and distrust in customers. This has happened in various shops from fast food restaurants to prominent retailers. Often, it's not that they don't have terminals in place. This may be due to inadequate onboarding, lack of proper staff training, difficulties in migrating some functionality, to streamlining the process to work their established tallying systems, some existing companies might still find it easier to only take cash as a means of purchasing. A note worth noting is due to user demand as well. The vendors could have set up the terminals, but if not many Malaysians are actually using cashless, then merchants really have no reason to leave the option enabled.

Accessibility for All

Smartphones are no longer luxury items as it became a necessity to most people as the penetration of smartphones is quite high and it is expected to be growing exponentially. However, there are some minorities who do not own and coping well without a smartphone. Are we leaving and side-lining these people behind? There are people who do not own a smartphone with various reasons- illiterate, financial issues and un-tech savvy etc due to old age, education and financial background? The obvious losers would be those of the aging population who are slower to absorb information about new technologies, at their age or even younger people who might not have bank accounts yet. Then, there are also those who are of a lower income, who often get paid purely in cash. People who are unbanked or who don't have enough money to start a bank account are automatically discriminated against when a society goes cashless. On the other hand, lower income people will not be able to afford to own a high-end mobile phones, with system that support these apps. It would be an additional burden for this category of people. Is it really fair to impose these technologies which they do not need or do not to embrace on their shoulders? Is it fair to say "We need to keep abreast with changes in order to stay ahead and those who do will be left behind" for every case as being treated fairly is what the world is trying to reach today.

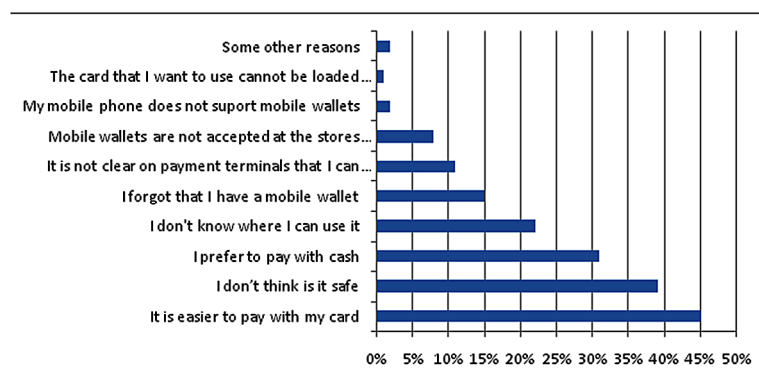
Cashless may be the new upcoming trend in the future, due to its convenience but there seems to be many issues starting from technicality to consumers' need to be addressed before the "cashless" can take over from the plastics as it does not seem to be a need and it is not necessary to go totally cashless in transactions. Although many countries do not have much need to adopt this system, but many are trying to go down this path in order to keep up to date with the current technological trends. A study was conducted in United States at 2017 on the reasons why consumers are not using e-wallet. Figure 4 illustrates the statistic on barriers to digital wallet adoption according to consumers in the United States as of November 2017. During the survey period, it was found that 39 percent of non-mobile wallet using respondents were hesitant to use digital wallets due to security concerns (The Statistical Portal, 2017).

CRIMES RELATED TO E-WALLETS

As stated earlier, one of the most concerns of e-wallet is its security. Due to cashless world and concept, there has been a new and on-going evolution of crimes pertaining to online payment for the cashless society. A new technique has surfaced in which hackers and fraudsters are siphoning money through people's e-wallets using phishing techniques. A hacker can trick a user into downloading a modified or

Figure 4. The statistic on barriers to digital wallet adoption according to consumers in the United States as of November 2017

Source: The Statistical Portal, 2017



a disguised version of the e-wallet applications by offering free credits and money which could be hiding hard-to-detect computer viruses like a Trojan. Besides losing the money in the e-wallet, users are very concerned about exposing personal information which can be obtained when registering for the e-wallet and even giving the hackers full access of your phone remotely. Mobile phones are considered a must-have item and a treasure full with personal passwords, personal notes as well as credit card and log-on details and the stakes are growing exponentially as the time goes. The growing and tempting stakes cause the continuous growth of cybercrimes around the world.

THE ANNUAL PAYMENT TRANSACTION USING E-WALLET

The annual payment transactions in US billion dollars from year 2015 to year 2021. The data for year 2018-2021 are projected. Figure 5 gives information on the proximity mobile payment transaction value in the United States from 2015 to 2021, in billion U.S. dollars. In 2021, near-field-communications or other contactless technologies are projected to generate close to 190 billion U.S. dollars in transaction value. As of 2015, about 12.7 percent of smartphone users in the United States were actively using proximity mobile payment services. Industry experts project mobile proximity payments to be amongst the most successful future mobile payment methods. Popular application areas are paying for transport and transit, as well as retail goods and services. According to a survey of digital payment users, the most common mobile in-store mobile payment method was barcode or QR code scanning and a further 12 percent had waved or tapped their mobile phone to pay at check out. Mobile wallet apps are used to facilitate mobile payments. PayPal, Google Wallet and Apple Pay are amongst the most popular digital wallet services according to users in the United States. A current example of mobile proximity payment usage is Starbucks. The coffee retailer allows customers to pay via mobile app by waving their phone at the checkout counter. Starbucks processes more than 8 million weekly mobile app payments, which account for 16 percent of all transactions.

Figure 5. The statistics on barriers to digital wallet adoption according to consumers in the United States as of November 2017

Source: The Statistical Portal, 2017

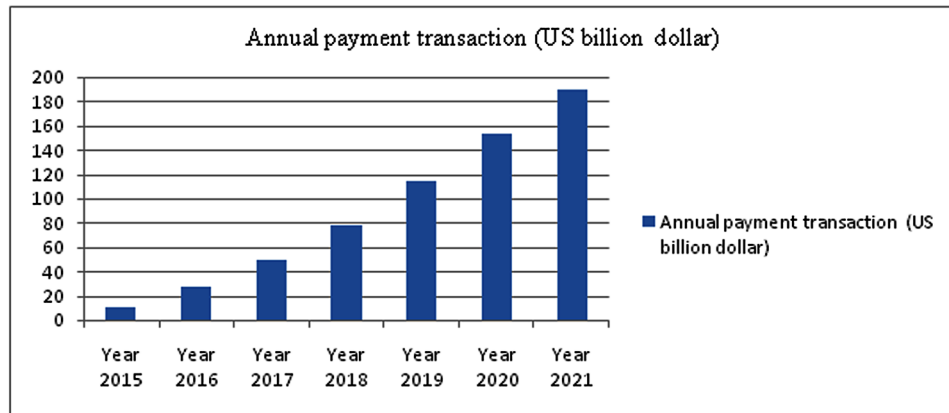
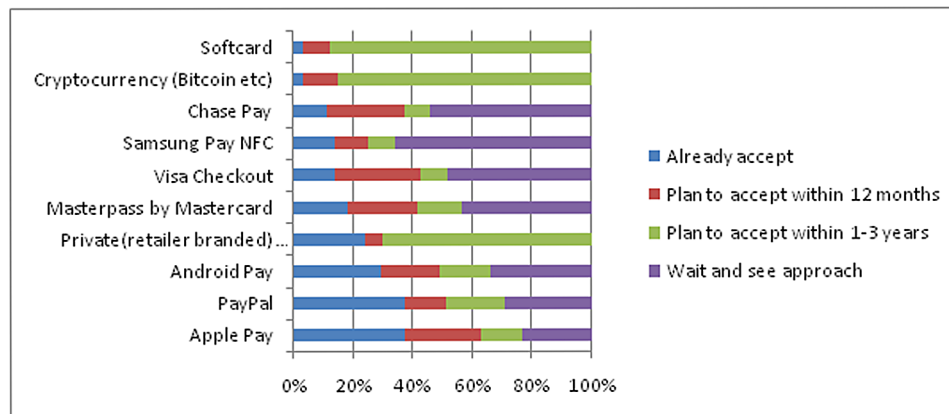


Figure 6: Digital payment methods by North American retailers as of December 2017

Source: The Statistical Portal, 2017



THE INTENTION TO ACCEPT THE DIGITAL PAYMENT METHODS BY RETAILERS

Based on a study in North America as of December 2017, we can see that 37 percent of responding North American retailers was already accepting customer payments via PayPal with 14 percent planning on accepting the payment method within the next 12 months. Figure 6 presents the most common digital payment methods that North American retailers accept or plan to accept. Mobile payments have become increasingly main stream in the United States as an increasing number of users take advantage of the conveniences of digital payment options. Scanning barcodes or using mobile apps are the most popular mobile payment methods among U.S. users. More than 12 percent of mobile payment users have purchased goods at a store using their mobile device. Mobile proximity payments enabled through near-field-communications (NFC) are also projected to vastly increase to 118 billion U.S. dollars in

2018, up from 3.5 billion U.S. dollars in 2014. According to industry professionals, mobile proximity payments are one of the mobile payment types most likely to succeed. According to smartphone users in the United States, mobile payments are a convenient way to pay for many reasons. Some of the benefits of mobile payments include the speed of payment, the convenience as well as the integration with pre-existing loyalty and coupon programs. Another well-received advantage of mobile payments was the ability to pay without sharing financial data with retailers.

THE FUTURE OF E-WALLETS

Due to its many setbacks and challenges of e-wallets, the future for mobile wallets is hazy at this point, although it seems hard to believe that in an increasingly wired world that more and more payments might migrate to digital channels. The peer-to-peer payment platforms like Venmo and Zelle have been well-received by consumers, however inertia is a powerful force, and change doesn't come easy. Change would not be easy unless it proves a total new breakthrough from the current practice. While digital payments are steadily growing in popularity, cash remains very much a part of consumers' financial lives, even in the least cash-friendly countries, perhaps due to the fact that physical cash provides a "sense of security" that virtual cash could not. With the rise of "cashless" world, it seems to have the tendency to sideline the minorities' purchasers such as the illiterate and financially poor purchasers.

Some users would perceive that mobile wallets would not be a widespread adoption phenomenon since it does not seem to solve the consumer problem and consumers may not want to make it as a habit to use e-wallets. Therefore, the road for e-wallets would not be an easy one. Nevertheless, consumers can be convinced rather easily when it involves monetary benefits. Loyalty programs will be a significant driver in retailer mobile wallet adoption.

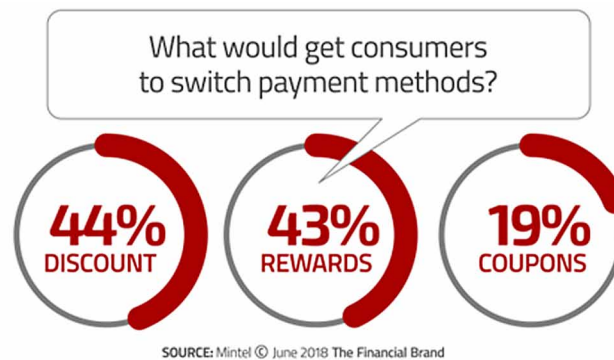
SOLUTIONS AND RECOMMENDATIONS

E-wallets have great potential to take over the transactions world if the setbacks and challenges are mitigated. There are still worries and doubts by many consumers by the term "virtual payment". The most common reasons why consumers are reluctant to adopt mobile payments are:

- It's not available at stores
- I would want to use it
- Technology doesn't always work properly
- I don't know which app is the best
- Credit cards have better rewards
- No single payment system across merchants
- Not as convenient as using cash or a credit card
- I don't want the store to have my mobile wallet info.
- I don't want to pay any fees
- I am worried about security
- The mobile screen is too small to make transactions

Source: CMB Consumer Pulse (2015)

Figure 7. The methods to increase adoption of mobile wallets as of June 2018
Source: Mintel, 2018



SOLUTIONS FOR CONSUMERS' CONCERNS ON E-WALLET CRIMES

- Fear of losing personal information from smartphone theft is the main fear for users. Enhancing the security software and ensure contingencies and refunding the money to purchasers' mechanism with convenience is in place. Priority should be given to the purchasers in order to gain their trust and also provide a sense of security to them.
- Integrate the same categorized payment platforms under one roof instead of several different apps which can be a nuisance to consumers
- Provide alternative payments for various consumers especially those who are illiterate, not tech-savvy consumers
- Ensure the payment terminal is in place and adequate trainings are provided as it can provide an assurance to the users.
- Easy account set-up for first-time users as this can hinders many potential users to walk-away from mobile wallet and tend to look back to physical cash payment.
- Provide more types monetary benefits to users. According to a study by Mintel (2018), it presents a significant opportunity for financial marketers looking to increase adoption of mobile wallets where discounts, rewards and coupons could get consumers to switch their payment type over to mobile wallets. Refer to Figure 7 for the methods to increase adoption of mobile wallets.

CONCLUSION

Consumers have split views on the future of cashless society. Some think that payments will become completely cashless within their lifetime as digitalization of payments can be considered as a boon to growth of a country's economy, while some do not share the same view as half of those believe that cash will disappear within the next five years. There can be more concentrated effort to bring users on board with mobile payments. E-wallets is a double-edge sword as on one hand, it provides the convenience to its users as it records all the payments from the amount, products and place and everything and it enables the consumers to track its expenses and manage his/her finance better. However, on the other hand, it is also a worry to users as it records everything about his/her spending patterns, favourite

place to dine, shop etc. All this information can be lethal to users if it falls into the wrong hands. The mobile wallet market is still evolving with no clear competitors claiming a definitive win. However, familiarity and comfort with online payments have translated to high awareness and satisfaction for a number of providers. According to Bluefin (2017), the mobile wallet marketplace remains fragmented and customers remain loyal to traditional forms of payment, mobile loyalty cards will lead the way toward a consumer landscape driven by mobile wallets. By 2020, transactions made using mobile wallets will reach \$503 billion.

FUTURE RESEARCH

A lot of security aspects are still left unexplored in this context. Information technology has to work hard towards making the transactions secure and complete as this is one of the major hindrance in the success of digital payments. One worthy note is that the possibilities of all the e-wallet providers to have a unanimous perspective how e-wallets can be implemented with a tighter and stronger security features. Other than that, the possibilities of mobile wallets could be introduced in transportation services in busses as a lot of cash transaction is involved on daily basis can be further explored. There is a need to address the gaps that exist between what customers want and what are being offered to them by merchants.

REFERENCES

- Consumer Pulse, C. M. B. (2015). *The Future of the Mobile Wallet: Barriers and opportunities for the next stage of the mobile payment revolution*. Retrieved from https://www.cmbinfo.com/assets/PR_Consumer-Pulse_MW_2015-min.pdf
- Mintel. (2018). *Why Mobile Wallets Are Struggling*. Retrieved from <https://thefinancialbrand.com/73332/future-mobile-wallets-payments-trends/>
- The Bluefin. (2017). *The Future Trends of Mobile Wallet Technology and the Role of Payment Security*. Retrieved from <https://www.bluefin.com/bluefin-news/future-trends-mobile-wallet-technology-role-payment-security/>
- The Financial Brand. (2018). *Why Mobile Wallets Are Struggling*. Retrieved from <https://thefinancial-brand.com/73332/future-mobile-wallets-payments-trends/>
- The Statistical Portal. (2017). *The Statistical Studies on Digital Payments*. Retrieved from <https://www.statista.com/statistics/722213/user-base-of-leading-digital-wallets-nfc/>
- Thrive Analytics. (2018). Retrieved from <http://www.thriveanalytics.com/Press%20Releases-%202014%20Digital%20Wallet%20Usage%20Study.html>
- Vulcan Post. (2017). *5 Challenges FavePay & Other Cashless Wallets Must Overcome To Grow In M'sia*. Retrieved from <https://vulcanpost.com/620539/challenges-ewallet-cashless-malaysia/>

Preliminary Insights Into the Adoption of Bitcoin in a Developing Economy: The Case of Ghana

Frederick Edem Broni

University of Ghana Business School, Ghana

Richard Boateng

 <https://orcid.org/0000-0002-9995-3340>

University of Ghana Business School, Ghana

Acheampong Owusu

 <https://orcid.org/0000-0001-7789-5162>

University of Ghana Business School, Ghana

INTRODUCTION

In this technological age, there exist different innovative money payment systems through which financial transactions are made possible and many of these money payment systems are built to run on platforms such as the Web and smartphones (Nian, Lee, & Chuen, 2015). These money payment gateways have enjoyed a continued growth, from the likes of SlydePay, ZeePay, Skrill, BitPesa, Apple Pay, Google Wallet, M-Pesa, BitPay and PayPal (Nian et al., 2015). In ensuring secured transactions on these platforms, the phenomenon of cryptocurrency is emerging. According to Nakamoto (2008), transactions on the web has come to depend exclusively on Financial organizations filling in as trusted third parties to process electronic installments. In spite of the fact that these frameworks work well for most electronic exchanges, it keeps on suffering from the genetic shortcomings of the trust-based model which are also known as “third-party based” payment processing systems. Contracts entered by trading parties are not enforced by these “trust-based” or “third-party-based” payment processing systems (Master Card, PayPal, American Express, SlydePay, and so on). Since contracts entered are not enforced by these trusted third-party payment processor, additional costs are being incurred by trading parties in their quest to ensure that the trade executed is based on the terms of the contract (Knott, 2013).

A Cryptocurrency is a digital or virtual currency that uses cryptography which changes data into a mystery code for transmission over an open system for security and was the first truly decentralized and digitized modern money (Nakamoto, 2008). With the use of special cryptographic techniques, signatures and also an incredible rewarding system, one can say that cryptocurrency is unlike any currency in the world. It requires no third parties such as the banks, credit card companies and others, just a peer-to-peer transaction which means from the sender directly to the receiver (Lee, 2013). Bitcoin is one of the cryptocurrencies in the world. It first appeared online in January 2009. The creator was a computer programmer under the name Satoshi Nakamoto. His open source invention was peer-to-peer which meant transactions did not require an intermediary like Skrill or PayPal to function but rather be electronic with absolutely no physical involvement. Unlike traditional money, Bitcoins exist only online, and they are

DOI: 10.4018/978-1-5225-9715-5.ch064

not considered as legal tender. Also, Bitcoins are not backed by any government or any legal entity, and their flow is not controlled by a central bank. With no third parties involved in transactions, the Bitcoin system is a very private one (Elwell, Murphy & Seitzinger, 2013).

This new mode of online financial transactions with bitcoins has transformed the perception of money in the form of traditional money as paper, coins, cheques, treasury bills, and so on, into seeing it in the form of mathematical money as digital ones and zeros or bits (Antonopoulos, 2015). In April 2016, the highest interest shown by African countries in bitcoins was Ghana. Ghana was ranked at number one with 100% interest in Africa (Scott, 2016). The creators of Dogecoin (a cryptocurrency) donated \$342 USD to the Ghana Medical Help (2016) to purchase medical equipment. They also created a Cryptocurrency Endowment Fund to accept donations from donors using cryptocurrencies (Ghana Medical Help, 2016).

Kubát (2015), hailing the innovativeness of Bitcoin, revealed that, judging from the opinions of the respondents, majority considered Bitcoin as a positive mode of transaction. They were optimistic that Bitcoin would represent a decentralized and a virtual new currency that would be out of the control of any governmental agency. Bitcoin is therefore a cheaper way to spend money even across national borders. Majority of e-commerce sites accept Bitcoins. In addition, many Bitcoin ATMs have been opened and one can even pay for college tuition fees with it. Bitcoin is like gold, but in a virtual environment (Rogojanu & Badea, 2014).

Bitcoin offers a secured mode of transaction. For instance, only owners of Bitcoin wallets can change their Bitcoin address. No hacker can illegally get access to Bitcoins unless they have direct access to the user's computer. Again, the Bitcoin system requires physical access unlike traditional currency where only a few verification steps are required to gain access to the account, which makes it almost impossible to hack (Dwyer, 2015).

With the fast growth of Bitcoin transactions, initial literature reviewed espoused that Bitcoin usage and its activities have gained considerable traction in developed countries and also that it is gaining grounds in some developing countries in Africa, Ghana included (Scott, 2016). The proposed research will therefore attempt to explore the adoption and usage of the Bitcoin technology among citizens of a developing country such as Ghana.

Over the years, users of fund transfer services and payment services have had to contend with unfavourable circumstances in the hands of middlemen (such as bank, a credit card company, and the telecommunications companies (Telco's) via m-payment systems) who hide behind these virtual services during business transactions. Sending funds to another person attracts high transactional fees and the total amount sent to the receiver is decreased on arrival (Dwyer, 2015). Elwell et al. (2013) concluded that Bitcoin transactions are to be significantly less expensive for users as compared to other traditional payment systems. Banks and Credit card companies for instance will charge merchants significant fees for their role as a trusted third-party intermediary in validation of an electronic transaction. Again, Njuguna (2014) found out that BitPesa is one of Africa's first Bitcoin startup that is making transfer of money from Kenyans living in UK to their loved ones in Kenya more efficient and possible. Extant studies (Kubat, 2015; Bonneau et al., 2015; Elwell et al., 2013; Dwyer, 2015; Singhal & Rafiuddin, 2014) have also looked at how cryptocurrencies have digitized and decentralized the modern currency system. Again, studies (Nakamoto, 2008; Nian et al., 2015; Njuguna, 2014) have looked at how Bitcoins are made and used, how beneficial it is to its users, and how its adoption has helped eased transactions locally and internationally? However, while there is a significant amount of evidence that Bitcoin actually cuts down on the cost of funds transfer across the world, arguably, there exists little or no comprehensive data on its existence, adoption, usage and its cost advantage from a developing country perspective.

The proposed research is exploratory since Bitcoin in the Ghanaian community is at its duding stage and is gradually gaining recognition in the Ghanaian marketplace. Many people in the country do not know what this great innovation is (Njuguna, 2014). As a result of the challenges in the adoption of Bitcoin, relevant guidance is needed to help individuals tap into the massive benefits of using Bitcoin. The usage of m-payment services in the country have skyrocketed. This means that there is need for researchers to explore challenges in the adoption of cryptocurrencies in the country.

The purpose of this study is to explore the determinants of Bitcoin adoption in Ghana and to assess the nature of the usage of the Bitcoin technology payment preferences in transactions.

The following outlined objectives will be achieved by the research:

1. To explore the nature of Bitcoin adoption in Ghana
2. To explore the determinants of bitcoin adoption as a payment option in Ghana

The following are the research questions asked:

1. What is the nature of Bitcoin adoption in Ghana?
2. What are the determinants of Bitcoin adoption as a payment option in Ghana?

The significance of this study can be investigated along research, policy, and practice. It will be critical to help contribute to the current learning bank of Bitcoin literature.

This study is to explore the determinants of Bitcoin adoption in Ghana and to assess the nature of the usage of the Bitcoin technology payment preferences in transactions. The Chapter is organized into five sections. The first section is the introduction to the chapter. The second section presents an overview Bitcoin and the Blockchain, advantages and disadvantages of Bitcoin, related work on Bitcoin and the research framework as well as the research methods used in the chapter. The third section deals with the data presentation, analysis of findings and discussion. The fourth section presents future studies directions. The last section deals with precis of the studies, implications (and suggestions) to investigate, practice and policy.

BACKGROUND

Bitcoin and the Blockchain: An Overview

Cryptocurrency was initially introduced at a time of economic instability (Ross, 2015). Over the years, Bitcoin, has been one of the interesting phenomena in the world (Kubát, 2015). Bitcoin was created with the aim of simplifying and solving transactional problems online.

Bitcoin is a decentralized payment scheme that facilitates peer-to-peer transactions between users; it allows user “A” to transact with user “B” directly without any third party involved (Thukral, 2017; Nakamoto, 2008) without depending on shared trust. The Bitcoin system has no incorporated issuing party. The information of every one of these exchanges, in the wake of being approved with a proof-of-work system, is gathered into what is known as the Blockchain. The system is customized to expand the cash supply in a gradually expanding geometric arrangement until the point when the aggregate number of Bitcoins achieves a furthest utmost of around 21 million BTC’s (Nakamoto, 2008).

Table 1. Sample related studies on bitcoin adoption

Article	Theory	Country	Sampling & Method	Adoption Determinants
Ermakova et al. (2017)	Diffusion of Innovations	Germany, Austria, Switzerland, UK, USA and Israel	Mixed Methods: empirical survey of around one hundred Bitcoin Experts	Anonymity and security Absences of central point of trust Theft or loss of Bitcoins Unpredictability and insecurity of the Bitcoin system
Folkinshteyn & Lennon (2017)	TAM	USA	Qualitative: a detail-rich in-depth single case developed from direct interviews conducted by the authors with the founder of blockchain startup Bidbit.	Perceived ease of use Perceived Usefulness Perceived risk
Zarifis et al. (2015)	Digital Currency Trust Model	Europe and North America	Quantitative: 562 Online Buyers	Trust
Njuguna (2014)	Diffusion of Innovations	Kenya	Qualitative: case study	Lower transaction costs Increased privacy Long term protection of loss of purchasing power from inflation

The Blockchain aids the Bitcoin framework to maintain a worldwide, freely conveyed record of exchanges, which is kept up through an algorithm running over a substantial number of Personal Computers appropriated over the world. These PCs play out a computationally intricate task called mining, which incorporates the exchange into the Blockchain. The transaction to charge from the sender's record and credit to the receiver's record is totaled with other pending transactions together into a block by one of these machines and presented on the top of the Blockchain (Nakamoto, 2008).

Advantages and Disadvantages of Bitcoin

Bitcoin has a number of advantages and disadvantages that will influence its adoption. The advantages are: No inflation due to political forces, Peer-to-peer cryptocurrency network - where transactions are without no third parties, no boundaries - which makes it possible to send transactions across countries, low transactional costs, Anonymity, transparency, etc. (Ivaschenko, 2016). The disadvantages of Bitcoin coin are that, it is highly volatile, can encourage money laundry and used for other illegal activities like funding of terrorist groups and the purchases of illicit drugs (Ivaschenko, 2016).

Related Work on Bitcoin

Extant studies have explored Bitcoin adoption from various perspectives, although all at the individual level but in different geographic contexts. This includes Ermakova, Fabian, Baumann, Izmailov & Krasnova (2017) in Europe/North America (Germany, Austria, Switzerland, UK, Israel and USA); Folkinshteyn & Lennon (2017) in USA; Zarifis, Cheng, Dimitriou & Efthymiou (2015) in Europe and North America; and Njuguna (2014) in Kenya as shown in Table 1.

In addition, Bitcoin adoption has also been studied using various theories such as TAM, DOI, and Digital Currency Trust Model. Yet, results from these studies have been inconclusive. Arguably, in the case of developing economies, little literature about Bitcoin adoption exist, thus there is the need for more studies in developing countries context in order to understand this phenomenon. In relation to Table

1, adoption determinants in developing economies differ from the developed economies. For instance, whilst studies from the developed world looked at Anonymity and security, Absences of central point of trust, Theft or loss of Bitcoins, Unpredictability and insecurity of the Bitcoin system, Perceived ease of use and Perceived Usefulness, Perceived risk and Trust (Ermakova et al., 2017; Folkinshteyn et al., 2017; Zarifis et al., 2015), a study from a developing country context suggested lower transaction costs, increased privacy and long term protection of loss of purchasing power from inflation to be the main factors to the adoption of Bitcoin (Njuguna, 2014).

Again, from Table 1, most studies were conducted in Europe and North America, which are developed economies, whilst few have been conducted in developing countries. Therefore, this study employs a theoretical approach to investigate Bitcoin adoption from a developing economy's perspective by adapting the UTAUT 2 model.

RESEARCH FRAMEWORK

The UTAUT2 Model

The aim of this study was to examine the factors affecting Ghanaians' intention to adopt and use Bitcoin in their transactions. These indicators that may affect the adoption of the technology are illustrated in Figure 1.

The improvement of the Unified Theory of Acceptance and Use of Technology 2 model (UTAUT2) had its hypothetical establishment on the UTAUT model by including three (3) extra additions, to be specific, price value, habit, and hedonic motivation (Venkatesh, Thong & Xu, 2012).

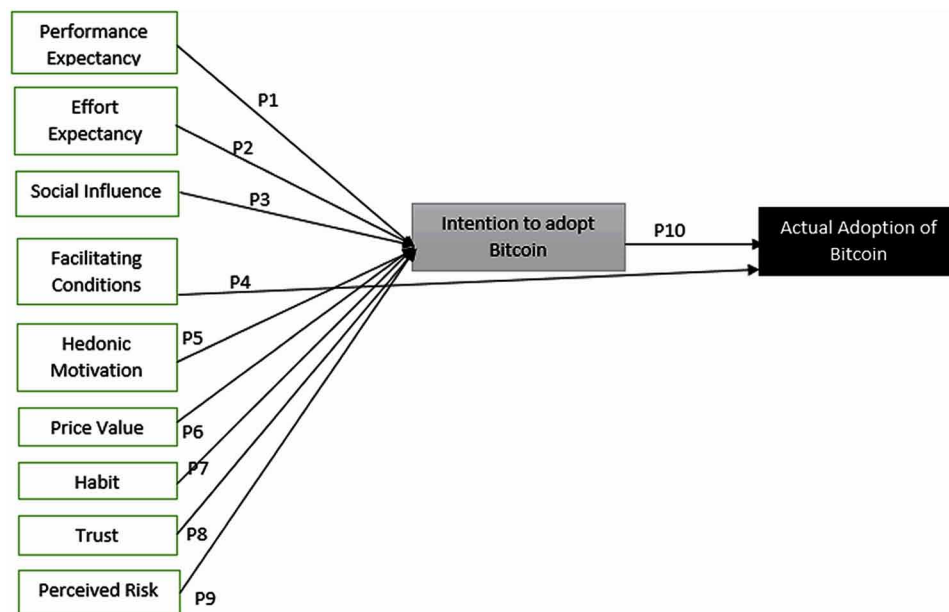
UTAUT2 and huge numbers of its forerunners were for the most part used to gauge the selection of data innovation frameworks (which examines info systems adoption). It includes the accompanying builds such as: Effort Expectancy, Performance Expectancy, Social Influence, Facilitating Conditions, Habit, and Hedonic Motivation (Roos, 2015).

Research Propositions

Performance Expectancy: This shows how much an individual assumes a technology or a system will be effective in the accomplishment of progresses in work execution (Venkatesh et al., 2012). It is the expectation of Ghanaians that Bitcoin will aid in the quick and successful completion of transactions. This will then make them have an intention to adopt Bitcoin. Zhou et al. (2010) found that performance expectancy has significant effects on user adoption of a technology. In another study, Chang, Yan & Tseng (2012) also found a significant effect of task technology fit on performance expectancy. Therefore, the researchers postulate that:

P1: Performance expectancy has a generally solid consolation on an individual behavioral aim in utilizing Bitcoin.

Figure 1. Bitcoin adoption framework



Effort Expectancy: This echoes the client's impression of the fact that it is so hard to utilize the innovation (Venkatesh et al., 2012). Ghanaians expect the use of Bitcoin to be smooth, easy and intuitive. They expect the utilization of Bitcoin to be user friendly. Effort expectancy is a significant predictor of the intention to adopt a technology (Deng, Liu & Qi, 2011). Also, Effort expectancy impacts the overall use of intention of a technology (Helena, Fang & Tseng, 2010). Therefore, the researchers postulate that:

P2: Effort expectancy impacts the behavioral expectation to utilize Bitcoin.

Social Influence: This is how much a person sees how colleagues, loved ones/individuals of huge significance assume that people should utilize the innovation (Venkatesh et al., 2012). Influence from other individuals using Bitcoin will help facilitate the adoption by Ghanaians. Venkatesh et al. (2003) stated that social influence significantly affects the adoption of a technology. Social influence also affects the acceptance of IT (Kijisanayotin, Pannarunothai & Speedie, 2009). Therefore, the researchers postulate that:

P3: Social influence impacts the behavioral expectation in utilizing Bitcoin.

Facilitating Conditions: This is how much a person assumes that a hierarchical and specialized framework (infrastructure) is set up to help utilization of the system (Venkatesh et al., 2012). The unique set of the Bitcoin network will aid the successful adoption by Ghanaians. Venkatesh et al. (2003) stated that facilitating conditions significantly affect the use of a technology. Therefore, the researchers postulate that:

P4: Facilitating conditions impacts the behavioral expectation to utilize Bitcoin.

Hedonic Motivation: This is another build included in the UTAUT2 model. Hedonic Motivation denotes the agony/delight realized from utilizing an innovation (Venkatesh et al., 2012). Ghanaians will adopt Bitcoin if they obtain a positive feeling as a result of using it. Yang (2010) found that hedonic motivation is a critical determinant of an individual's intentions to use a technology. Therefore, the researchers postulate that:

P5: Hedonic motivation positively influences an individual's behavioral expectation in utilizing Bitcoin.

Price Value: This refers to the tradeoff between the benefits of a good or service and the monetary cost of that particular good or service (Venkatesh et al., 2012). The price value of the technology will influence Ghanaians to adopt Bitcoin. The cost and pricing structure may have a significant impact on consumers' technology use (Venkatesh et al., 2012). They also stated that the benefits of using a technology is much greater when the price value is positive than the cost, which will lead to a positive impact on intentions to adopt. In a study conducted by Njuguna (2014) about Bitcoin adoption in developing economies, it was found that the low transactional cost of Bitcoin significantly affects the intention of an individual to use the technology. Therefore, the researchers postulate that:

P6: Price value positively influences an individual's behavioral expectation in utilizing Bitcoin.

Habit: This is how much individuals tend to play out a conduct naturally due to an increased comprehension or learning (Venkatesh et al., 2012). Ghanaians will intend to adopt Bitcoin if it becomes a necessary requirement in purchasing some products online.

Therefore, the researchers postulate that:

P7: Habit influences an individual's behavioral expectation in the utilization of Bitcoin

New Constructs

To be able to accurately determine and explain why individuals adopt a technology from a developing economy's perspective, the researchers introduced two additional constructs to add to the existing model. Trust and Perceived risk were the extra constructs added to the UTAUT2 model by the researchers. Consideration of the development of the UTAUT2 model is bound by Bagozzi (2007) and Venkatesh et al's. (2007) submissions which wishes to extend the first model in order to utilize it in various settings (Roos, 2015).

Trust

Rousseau, Sitkin, Burt & Camerer (1998) stated that trust is an individual's readiness in relying upon other individuals gathering in light of their attributes. The eminent sociologist Georg Simmel asserted that trust is the premise of any financial request (Altmann, 1903).

In any case, researchers, for example, Komiak & Benbasat (2004) have seen trust from the passionate perspective and characterized it as the degree to which an individual feels secure and sure about depending on the trustee. Ennew & Sekhon (2007) have characterized trust as a person's eagerness to acknowledge defenselessness on the grounds of inspirational assumptions about the aims or conduct of another in a circumstance described by reliance and risk. This definition joins both the enthusiastic and intellectual

measurements of trust. Folkinshteyn & Lennon (2017) in a study about Bitcoin adoption found out that trust is highly important during transactions between the two parties. In this manner, Ghanaians trust that the Bitcoin infrastructure is secured, and level of risk associated with it is minimal, hence aiding in its adoption. In another study, Zarifis et al. (2015) also found that trust is very essential and affects the adoption of digital currencies of which Bitcoin is part of. Therefore, the researchers postulate that:

P8: Trust positively influences an individual's behavioral expectation in utilizing Bitcoin.

Perceived Risk

Perceived risk in a user's conduct is characterized as any activity of a buyer that may prompt offensive results (Lopez-Nicola's & Molina-Castillo, 2008). Different investigations have considered perceived risk as the user's expectations of misfortune in quest for a desirable result. In light of the previous definition, perceived risk is a multidimensional construct comprising of four measurements: budgetary(financial), mental, execution and social misfortune (Ho & Ng, 1994; Keat & Mohan, 2004; Lu et al., 2005) or danger of losing individual control (cash, time) and danger of framework disappointment.

Nonetheless, Pavlou (2003) and Shin & Kim (2008) in their findings, contend that hazard ascends from people subjectively and is hard to catch unbiasedly. The division of perceived risk into sub-measurements in some cases are not precise and can't survey all the applicable danger measurements, particularly when the study concentrates on unsafe systems like transacting online (Wanget al., 2003). Ermakova et al. (2017) in their study found out that perceived risk of theft or loosing Bitcoins through an attack or due to human error negatively affects an individual's ability to adopt the technology. Perceived risk of loss as a result of dishonesty due to the use of bitcoin heavily affects the adoption of the technology (Folkinshteyn & Lennon, 2017). Therefore, the researchers postulate that:

P9: Perceived Risk positively affects the behavioral expectations in utilizing Bitcoins.

P10: Intention to adopt Bitcoin directly influence the Actual adoption of Bitcoin.

Methodology

The proposed research utilized the qualitative approach through interviews. Due to the exploratory nature of this phenomenon, the qualitative approach was deemed fit, hence its usage.

The reason for using this instrument is to track the perceptions of Ghanaians who use bitcoins and to assess their level of knowledge and also discover challenges faced by them.

The target population for this study was bitcoin community in Ghana. The sampling method used was purposive sampling since it is extremely difficult to find bitcoin users especially in Ghana. The convenience sampling made use of respondents who were available and willing to partake in the study.

Data Collection Methods

The method of data collection for this research was evaluation of primary and secondary data which included academic journals, thesis and reports published previously. The instruments used for the data collection were interviews and phone calls.

The essential information sources included twelve (12) respondents, from educational institutions and industrial conferences involved in Blockchain and Bitcoin development in Ghana. These respondents consisted of three faculty members, two bitcoin traders, one blockchain developer, one financial expert, and five student entrepreneurs. The interviews were recorded, transcribed and presented to respondents to make corrections where necessary.

Data Analysis

The evidence gathered were presented in relation to the constructs of the model. This allowed for the easier drawing of themes from the response gathered from the respondents. This enabled the researcher to map out similarities and contrasts from the results obtained in relation to the adoption of bitcoin.

SOLUTIONS AND RECOMMENDATIONS

Findings and Discussion

The purpose of this study was to explore the determinants of Bitcoins adoption among Ghanaian individuals and to assess the nature of the usage of the Bitcoin technology payment preferences in transactions.

Respondents judged the use of Bitcoin as extremely positive. Regardless of the moderately low awareness rate, all respondents showed that they will keep utilizing Bitcoin on the premise that the effort expected to utilize it, the facilitating conditions and the performance of the use of Bitcoin will continue as before.

The principal concern communicated by the few respondents were the value fluctuations of Bitcoin. Despite the fact that they saw Bitcoin to have certain advantages over other payment methods, a few respondents expressed that Bitcoin represented some type of hazard in its use, which in this way affected their choice to keep utilizing it. This study explored the hypothesis that the greatest difficulty confronting Bitcoin appropriation among prospective users was the assumed challenges as regards understanding the idea of Bitcoin and how it can altogether decrease the cost of exchanges.

Another worry of a few respondents on the issue of trust were featured as powerless focuses for the appropriation of Bitcoin. Trust was found as an essential prerequisite for the proposed continuation to utilize Bitcoin.

Most respondents likewise esteemed decidedly the Price estimation of Bitcoin. They communicated they want to utilize it more because of the way that the estimation of Bitcoin continues expanding due to its appeal. Heintze (2014) said this enables them to accumulate Bitcoins to push the costs up in view of speculations.

Performance Expectancy

Three topics related to the performance expectancy of Bitcoins were mentioned. Quick transactional operations were one of the three most frequently mentioned by the respondents. They expected that since transactions are peer-to-peer, it will increase the effectiveness of Bitcoins and enhance its usefulness.

However, the perceptions of the respondents concerning the fulfilment of these expectations were very diverse. Respondents were positive about the added value of the use of Bitcoins:

Due to the use of Bitcoins, I am able to do transactions faster by just scanning the QR code of the recipient address, which definitely saves time and its of added value.

Improved productivity: Respondents expected to accomplish tasks more quickly and consequently achieve an improved productivity by the use of Bitcoins. A respondent stated:

Bitcoin offers one thing that anyone can hope for, that is the freedom to perform transactions without worrying about limitations. I am able to do more transactions with bitcoins in less time.

This idea came about from the expectation that the Bitcoins enable faster transaction processing which ensures the ability of users to process more transaction, which should have been less time consuming.

A cost-effective application: Respondents claimed that Bitcoins should be of added value when using it and that possible financial benefits of the Bitcoins would play a major role in the actual use of the currency. However, all respondents who valued the cost-effectiveness of Bitcoins revealed that it is very cost-effective and profitable. A respondent indicated:

The cost of transactions when using bitcoins is very low compared to other payment options.

As seen in our study, it has been established that Performance expectancy has been a major influencing factor which significantly affects the intention to adopt Bitcoin. This was affirmed by studies conducted by (Zhou et al., 2010; Venkatesh et al., 2012; Chang, 2012) where it was found that performance expectancy significantly affects an individual's ability to adopt and use a technology.

Effort Expectancy

Alongside the performance expectancy of the use of Bitcoins, some topics related to the effort expectancy of the use of Bitcoins were discussed. Respondents mentioned the user-friendliness of Bitcoins as one of the requirements for their intended continuation to use it.

Learning to use the Bitcoins: The effort expectancy of the respondents related to this topic was relatively low. For example, a respondent said:

There was no difficulty when learning to use Bitcoins. It was user friendly and I could operate it on my own with the little assistance given by the Bitcoin wallet application, which did not require any special IT knowledge.

However, there was no consensus about the actual effort needed to learn how to use Bitcoins. Respondents stated these differences to the amount of IT experience and the user-friendliness.

Daily use of Bitcoins: The effort expectancy regarding the daily use of Bitcoins was also relatively high. For example, a respondent said that:

I expected the Bitcoins to be easy to use. Using it was clear and I really understood how it works.

The actual effort needed to access and use Bitcoins daily was very little:

I don't struggle when using Bitcoins and you don't spend a lot of time using it. Everything is fast and simple.

Another respondent said:

The experience has rather been much more effortless.

Effort expectancy in the use of Bitcoin was very important and was found out that it significantly influences an individual's intention to adopt and use Bitcoin. This is in line with the findings from studies (Helena et al., 2010; Deng et al., 2011; Venkatesh et al., 2012) which revealed that Effort expectancy is a major predictor and significantly impacts the behavior of an individual in IT adoption and innovation.

Social Influence

With this construct, two different topics were discussed during the interview about the social influence of Bitcoins.

First of all, the view of colleagues and clients regarding Bitcoins was very diverse. The difference in opinions might be related to the local clients. A respondent indicated that:

My colleagues use bitcoins to increase value since the value of bitcoins is rising every day and I also noticed that Bitcoins was mainly useful when I am not doing physical transactions like paying for stuff overseas. Its less useful for local clients or clients that I physically meet to transact business with.

Respondents were also asked about the importance and influence of the views of colleagues and clients on their own opinions. The respondents confirmed the importance and influence on their own opinions as opposed to a minority of the respondents who expressed a different view:

All my colleagues who are using bitcoin mostly feel the same way I do. They speak highly of it and it encourages me to use it even more. The opinions of my colleagues are important, in the sense that they give me more information on the market value of bitcoins and whether to buy more or less coins because some of them are Bitcoin merchants.

Another respondent stated:

I'm still learning new things about bitcoins. My organization has also been helpful and provided invaluable motivation.

Almost all respondents felt supported by their colleagues and clients. This support was in the form of information sharing about the value of the coins and other Bitcoin investment opportunities. In this study, Social influence has been recognized as an influencing factor in Bitcoin adoption as confirmed with studies (Venkatesh et al., 2003; Kijisanayotin et al., 2009; Venkatesh et al., 2012) which also found out that Social Influence significantly influences the adoption of a technology.

Facilitating Conditions

Most topics which were mentioned by the respondents during the interview related to the facilitating conditions of Bitcoins.

Resources and knowledge necessary to use Bitcoins: It was remarkable that the respondents possess knowledge as well as the resources necessary to utilize Bitcoins. Moreover, a respondent mentioned to have had the knowledge, but not the appropriate device to use Bitcoin.

I lost my smartphone and had no computer; therefore, I shared a computer with a colleague who was my roommate. I did receive an android phone running OS 4.0, but the Bitcoins wallet application did not function properly on the android phone.

Attitude towards using technology: Respondents indicated to be very positive about working with technology. In addition, doing business with the aid of technology is the future according to them. A respondent stated:

Technology provides us with means to approach problems differently. It gives us different ways of solving complex problems more effectively and efficiently. In today's world, the use of technology has become a common practice because it helps boost productivity. I do a lot of buying online and websites nowadays have integrated various payment systems on their websites. That's how I noticed that Bitcoin wallet addresses or QR codes can be integrated with the site which would fit well with Bitcoin users.

Changed behavior: Respondents highlighted the fact that it was easier letting go of payment methods and developing a positive behavior towards the use of Bitcoins. This situation was as a result of the fact that they were looking for innovative and cost-effective methods of managing money transactions.

The knowledge and resources needed for Bitcoin, attitude to the technology and the behavior exhibited by an individual is very important for the actual use of Bitcoin. Facilitating conditions was found to significantly impacts and plays an important role in Bitcoin adoption in this study. This is consistent with studies (Venkatesh et al., 2003; Venkatesh et al., 2012) which found out that Facilitating Conditions emerged as a predictor and an influencer in adopting a technological innovation.

Price Value

Transactional cost: Respondents revealed that the cost incurred from Bitcoin transactions are relatively cheaper and reasonably priced which provides significant savings compared to other forms of payment. A respondent accounted that:

Currently there are either no fees, or very low fees within Bitcoin payments.

Benefits enjoyed from the usage of Bitcoin has been emphasized in studies as a major predictor of Bitcoin adoption. This study found out that price value was significant influencer in the adoption of the Bitcoin innovation thereby affirming the findings by (Venkatesh et al., 2012; Njuguna, 2014).

Hedonic Motivation

Feedback from clients: Respondents reported positive feedback from customers on how Bitcoin is easy to use; they found using it enjoyable and derived great pleasure when transacting with Bitcoins.

The user-friendly nature of Bitcoin makes it an enjoyable activity which provides satisfaction for an individual and actually impacts the intention to adopt the Bitcoin innovation. This study revealed that Hedonic motivation contributed for the adoption of Bitcoin hence affirming studies (Yang, 2010; Venkatesh et al., 2012) which also found hedonic motivation to be a significant influencer and predictor in technology adoption.

Habit

Respondents stated that the use of Bitcoins had not become a habit for them since most people do not recognize it here. Speaking of addiction, respondents quickly stated that they are not in any way addicted to Bitcoins and it is not obligatory that they use it for every transaction.

In this study, Habit was found not to be a predictor of the Bitcoin adoption from a developing economy's perspective. Individuals in developing economies tend to have a habit of using physical currencies for everyday transactions. This is in contrast with studies (Venkatesh et al., 2012) that found out that Habit significantly influences the adoption of the Bitcoin innovation. This is in relation to the lack of understanding and convenience on the part of retailers in developing economies. Paying for goods and services in developing economies are transacted with physical currencies and has become a habit of individuals in developing economies to rely more on the use of paper money to fulfil financial obligations.

Trust

Integrity: Respondents asserted the fact that since the bitcoin network is global and does not belong to a particular person, integrity is assured in the sense that transactions are recorded in a public ledger which is seen by everyone on the network. Thus, everything stays synchronized and nothing is altered. This makes the platform perfectly honest and truthful.

Personal Information: Personal details of the owners are not revealed to anyone. A respondent indicated that:

The owner has full control of his money because there is no central authority in the Bitcoin network. It gives you the freedom to have control over your own money. The fact that personal information is not required for transactions also influences my decision to opt for bitcoin for my transactions with the rise in internet fraud, it is necessary to protect any personal information whenever possible.

Trust in a system is very important indicator and predictor in the adoption of a technology (Rogers & Shoemaker, 1971). Trust in this study was found to be very essential for individuals and low levels of trust hinders the intention to adopt Bitcoin. This is true as studies (Folkinshteyn & Lennon, 2017; Zarifis et al., 2015) confirm that trust in a system ensures a successful adoption of Bitcoin therefore making it a significant factor in the adoption of an innovation.

Perceived Risk

Some respondents stated that transactions with Bitcoin are secure and safer than other forms of transactions. The security features in Bitcoin does not allow unauthorized use due to its cryptographic nature making it hard to break. A respondent said that:

In spite of the fact that Bitcoin is absolutely digital, it can be kept secure in analog form. Paper wallets can be utilized to store Bitcoins offline which fundamentally diminishes the odds of the cryptocurrency being stolen by programmers or PC infections.

Others were skeptical and felt insecure about it. A respondent said:

Well, yes, with the advancement of technology and hackers all over, I still have a little bit of reservations on how secured the platform can be.

It was found in this study that Perceived risk is an important contributor for the adoption of Bitcoin as a result of the secureness and how rigid the Bitcoin system is. This confirms the findings from studies (Wang et al., 2003; Ermakova et al., 2017; Folkinshteyn & Lennon, 2017) that suggested that perceived risk significantly influences the adoption of a technological innovation.

Intention to Use

All respondents proposed to keep utilizing Bitcoin on the premise that it was less expensive while doing exchanges, easy to use and straightforward, and was exceptionally secure compared with different types of payments. Besides, it was recognizable that an expanded profitability rate and an expanded viability of utilizing Bitcoin was deemed normal by respondents. Although, every one of them expressed to have the assets and learning important to utilize Bitcoin, yet some remarked adversely on its similarity issues. Moreover, it was interesting that respondents who needed to expand their utilization of Bitcoin were supported by their colleagues.

Also, it was surprising that most respondents had knowledge of Bitcoin and that all their hopes in terms of ease of use were met although the real push to utilize it was low.

Table 2 below summarizes the findings and provide lessons obtained from the findings:

FUTURE RESEARCH DIRECTIONS

Any research study, unavoidably, is expected to experience some limitations, and this research is no exemption. The following are a few limitations that have been distinguished in this study with proposed future research directions.

The study was restricted to Ghanaians in the capital city (Accra) as a result of the ease of finding respondents and information that the researchers expected to assemble. Consequently, future research ought to be completed utilizing a wider geographic area in Ghana. Also, this study adopted a qualitative approach interviewing twelve respondents thus making it difficult to generalize the findings in the Ghanaian context. In addition, the unit of analysis was done at the individual level. Future study can conduct a quantitative survey covering more firms to ascertain the adoption of Bitcoin at the firm level in Ghana.

Table 2. Lessons obtained from findings

Construct	Proposition	Lessons
Effort Expectancy	Effort expectancy impacts the behavioral expectation to utilize Bitcoin.	Effort expectancy in the use of Bitcoin was very important and was found out that it significantly influences an individual's intention to adopt and use Bitcoin.
Performance Expectancy	Performance expectancy has a generally solid consolation on an individual behavioral aim in utilizing Bitcoin.	Quick transactional operations, Improved productivity and a cost-effective application impacts on the intention to adopt Bitcoin
Facilitating Conditions	Facilitating conditions impacts the behavioral expectation to utilize Bitcoin.	The knowledge and resources needed for Bitcoin, attitude to the technology and the behavior exhibited by an individual significantly impacts and plays an important role in Bitcoin adoption
Social Influence	Social influence impacts the behavioral expectation in utilizing Bitcoin.	Social influence through information sharing about the value of the coins and other Bitcoin investment opportunities from colleagues and clients influences Bitcoin adoption
Habit	Habit doesn't influence an individual's behavioral expectation in the utilization of Bitcoin	Individuals in developing economies tend to have a habit of using physical currencies for everyday transactions.
Hedonic Motivation	Hedonic motivation positively influences an individual's behavioral expectation in utilizing Bitcoin.	The user-friendly nature of Bitcoin makes it an enjoyable activity which provides satisfaction for an individual which actually leads to the intention to adopt the Bitcoin innovation.
Price Value	Price value positively influences an individual's behavioral expectation in utilizing Bitcoin.	Transactional cost of Bitcoin encourages its adoption due to its cost effectiveness
Trust	Trust positively influences an individual's behavioral expectation in utilizing Bitcoin.	Integrity and the protection of personal information facilitates the adoption of Bitcoin
Perceived Risk	Perceived Risk positively affects the behavioral expectations in utilizing Bitcoins.	The secureness and the rigid nature of the Bitcoin system contributes significantly to its use.

Drawing from the findings of the study, the researchers recommend that policy makers (government) should provide a legal and regulatory framework in the implementation of a national policy on the use of bitcoins in the country.

CONCLUSION

This study seeks to investigate the nature of Bitcoin adoption in Ghana and also explored the determinants of Bitcoin adoption as a payment option in Ghana through the lens of UTAUT2.

Findings from our analysis indicate that majority of individuals in Ghana are aware of the Bitcoin technology and have considerable knowledge of how to use this innovation. This is so as the use of Bitcoin doesn't require much therefore individuals in the country are gearing towards its use. In addition, individuals, business owners and business partners preferred the bitcoin option as it reduces the cost of money transactions which allowed them to consider it as a payment method for international transactions. Also, availability to Bitcoin merchants in the capital city (Accra) allowed easy access to individuals who wanted to buy and sell their Bitcoin therefore encouraging the use of the technology.

Again, in this study, it emerged that the determinants of Bitcoin adoption in the Ghanaian context are Performance Expectancy, Effort Expectancy, Social Influence, Hedonic Motivation, Price Value, Trust

and Perceived risk. Evidence also showed that Facilitating conditions directly influence the actual adoption of Bitcoin. However, this study established that Habit had no effect on the intention to adopt Bitcoin.

Taking everything into account, the utilization of Bitcoin is considerably gaining recognition and enthusiasm in Ghana. This observation is affirmed by Ted Owusu Duodo (CEO of PMCedis Capital) who reveals that “the demand for bitcoin in Ghana is very high. But, in general, very few people know about Bitcoin. The people who are into it are mostly the youth and among them, the demand is very, very high” (Scott, 2016). It was additionally ascertained that Bitcoin decreases the cost of exchanges. Bitcoin were delivered as money to be free of any central authority, transferable electronically, pretty much in a split second, with low exchange expenses, when contrasted with conventional assets exchange administrations like Western Union and PayPal. Additionally, the challenges explored the appropriation of Bitcoin as another innovation basic to new advances. Significant mindfulness and preparation should be done to the potential clients of the innovation to ease utilization and diminish the protection from change that may be caused by dread of progress.

REFERENCES

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-T
- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.
- Altmann, S. P. (1903). Simmel’s philosophy of money. *American Journal of Sociology*, 9(1), 46–68. doi:10.1086/211195
- Antonopoulos, A. M. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O’Reilly Media, Inc.
- Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74–94. doi:10.1007/BF02723327
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Research perspectives and challenges for bitcoin and cryptocurrencies (extended version). *Cryptology ePrint Archive, Report 2015/452*.
- Chang, C. C., Yan, C. F., & Tseng, J. S. (2012). Perceived convenience in an extended technology acceptance model: Mobile technology and English learning for college students. *Australasian Journal of Educational Technology*, 28(5). doi:10.14742/ajet.818
- Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation). Massachusetts Institute of Technology.
- Deng, S., Liu, Y., & Qi, Y. (2011). An empirical study on determinants of web based question-answer services adoption. *RE:view*, 35(5), 789–798.
- Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81–91. doi:10.1016/j.jfs.2014.11.006

Elwell, C. K., Murphy, M. M., & Seitzinger, M. V. (2013). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Academic Press.

Ennew, C., & Sekhon, H. (2007). Measuring trust in financial services: The trust index. *Consumer Policy Review*, 17(2), 62–68.

Ermakova, T., Fabian, B., Baumann, A., Izmailov, M., & Krasnova, H. (2017). *Bitcoin: Drivers and Impediments*. Available at SSRN 3017190

Helena Chiu, Y. T., Fang, S. C., & Tseng, C. C. (2010). Early versus potential adopters: Exploring the antecedents of use intention in the context of retail service innovations. *International Journal of Retail & Distribution Management*, 38(6), 443–459. doi:10.1108/09590551011045357

Help, G. M. (2016a, March 14). *Cryptocurrency Endowment Fund*. Retrieved from Ghana Medical Help. Retrieved from <http://www.ghanamedicalhelp.com/>

Help, G. M. (2016b, January 28). *Thanks to Dogecoin for \$342-usd-for medical Equipment*. Retrieved from Ghana Medical Help: http://www.ghanamedicalhelp.com/blog_posts/thanks-to-dogecoin-for-342-usd-for-medical-equipment-purchasing

Ho, S. S., & Ng, V. T. (1994). Customers' Risk Perceptions of Electronic Payment Systems. *International Journal of Bank Marketing*, 12(8), 26–38. doi:10.1108/02652329410069029

Ivaschenko, A. I. (2016). Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to Improve their Investment Attractiveness. *Problèmes Économiques*, (3): 267–273.

Keat, T. K., & Mohan, A. (2004). Integration of TAM based electronic commerce models for trust. *The Journal of American Academy of Business, Cambridge*, 5(1/2), 404–410.

Kijsanayotin, B., Pannarunothai, S., & Speedie, S. M. (2009). Factors influencing health information technology adoption in Thailand's community health centers: Applying the UTAUT model. *International Journal of Medical Informatics*, 78(6), 404–416. doi:10.1016/j.ijmedinf.2008.12.005 PMID:19196548

Knott, A. (2013). *Bitcoin*. Retrieved from Panarchy Website: <https://www.panarchy.org/knott/bitcoin.html>

Komiak, S. X., & Benbasat, I. (2004). Understanding customer trust in agent-mediated electronic commerce, web-mediated electronic commerce, and traditional commerce. *Information Technology Management*, 5(1-2), 181–207. doi:10.1023/B:ITEM.0000008081.55563.d4

Kubát, M. (2015). Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value. *Procedia Economics and Finance*, 30(15), 409–416. doi:10.1016/S2212-5671(15)01308-8

Kuhn, T. S. (1962). The structure of scientific revolutions. *Journal of the History of the Behavioral Sciences*, 2, 274–276.

Lee, H. (2013). *Trends in Cryptocurrency: Understanding Digital Money*. Academic Press.

Lennon, M. M., & Folkinshteyn, D. (2017). From Bit Valley to Bitcoin: The NASDAQ Odyssey. *Global Journal of Business Research*, 11(1), 85–103.

Lopez-Nicola's, C., & Molina-Castillo, F.J. (2008). Customer knowledge management and e-commerce: the role of customer perceived risk. *International Journal of Information Management*, 28(2), 102–113.

Lu, H. P., Hsu, C. L., & Hsu, H. Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security*, 13(2), 106–120. doi:10.1108/09685220510589299

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Academic Press.

Nian, L. P., & Chuen, D. L. K. (2015). Introduction to bitcoin. In *Handbook of Digital Currency* (pp. 5–30). Academic Press. doi:10.1016/B978-0-12-802117-0.00001-1

Njuguna, M. E. (2014). *Adoption of Bitcoin in Kenya, a Case Study of Bitpesa*. Academic Press.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. doi:10.1080/10864415.2003.11044275

Rogers, E. M., & Shoemaker, F. F. (1971). *Communication of Innovations; A Cross-Cultural Approach*. Academic Press.

Rogojanu, A., & Badea, L. (2014). The Issue of competing Currencies. Case Study – Bitcoin. *Theoretical and Applied Economics*, 21(1), 103–114.

Roos, C. (2015). *The motivation and factors driving crypto-currency adoption in SME's*. Gordon Institute of Business Science. University of Petoria.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393–404. doi:10.5465/amr.1998.926617

Scott, A. (2016, April 11). *Interview: Is Ghana Showing the Most Interest in Bitcoin Right Now?* Retrieved from Bitcoin News: <https://news.bitcoin.com/ghana-interested-bitcoin/>

Shin, D. H., & Kim, W. Y. (2008). Applying the technology acceptance model and flow theory to cy-world user behavior: Implication of the web2. 0 user acceptance. *Cyberpsychology & Behavior*, 11(3), 378–382. doi:10.1089/cpb.2007.0117 PMID:18537514

Terre Blanche, M., & Durrheim, K. (1999). Social constructionist methods. *Research in practice: Applied methods for the social sciences*, 147–172.

Thomas, L. D., Vernet, A., & Gann, D. M. (2016). Adoption readiness in service innovation: The case of digital money. *Industry and Innovation*, 23(4), 353–381. doi:10.1080/13662716.2016.1156519

Thukral, S. (2017). Unfolding Bitcoin. *International Journal Of Research In Commerce & Management*, 8(2), 32–33.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly*, 27(3), 425–478. doi:10.2307/30036540

Venkatesh, V., Thong, J. Y., Chan, F. K., Hu, P. J., & Brown, S. A. (2011). Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context. *Information Systems Journal*, 21(6), 527–555. doi:10.1111/j.1365-2575.2011.00373.x

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *Management Information Systems Quarterly*, 36(1), 157–178. doi:10.2307/41410412

Wang, Y. S., Wang, Y. M., Lin, H. H., & Tang, T. I. (2003). Determinants of user acceptance of Internet banking: An empirical study. *International Journal of Service Industry Management*, 14(5), 501–519. doi:10.1108/09564230310500192

Yang, K., & Lee, H. J. (2010). Gender differences in using mobile data services: Utilitarian and hedonic value approaches. *Journal of Research in Interactive Marketing*, 4(2), 142–156. doi:10.1108/17505931011051678

Zarifis, A., Cheng, X., Dimitriou, S., & Efthymiou, L. (2015). *Trust in Digital Currency Enabled Transactions Model*. MCIS.

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, 26(4), 760–767. doi:10.1016/j.chb.2010.01.013

ADDITIONAL READING

Baur, A. W., Bühler, J., Bick, M., & Bonorden, C. S. (2015, October). Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co. In *Conference on e-Business, e-Services and e-Society* (pp. 63-80). Springer. 10.1007/978-3-319-25013-7_6

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2018). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*.

Presthus, W., & O'Malley, N. O. (2017). Motivations and Barriers for End-User Adoption of Bitcoin as Digital Currency. *Procedia Computer Science*, 121, 89–97. doi:10.1016/j.procs.2017.11.013

Shahzad, F., Xiu, G., Wang, J., & Shahbaz, M. (2018). An empirical investigation on the adoption of cryptocurrencies among the people of mainland China. *Technology in Society*, 55, 33–40. doi:10.1016/j.techsoc.2018.05.006

KEY TERMS AND DEFINITIONS

Bitcoin: A computerized and worldwide form of money. It enables individuals to send or receive cash over the web, even to somebody they don't know or don't trust.

Blockchain: A distributed record or database of exchanges recorded in a dispersed way, in a network of computers.

Cryptocurrency: A virtual cash intended to fill in as a mode of trade.

Cryptography: A strategy for encoding data in a specific way with the goal that those for whom it is planned can peruse and process it.

Payment Gateway: An online service that facilitates cashless transactions.

Peer-to-Peer: A distributed service whereby one person communicates with another, without intermediation by an outsider.

Proof-of-Work: An algorithm used to affirm transactions and produce new blocks to the chain.

Section 5

Security Tools and Solutions, Human-Based Cyber Defense, and the Social Understanding of Threats

The Importance of the Human-Centric Approach in Combating Cyber Threats

Pamela Goh

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Loo Seng Neo

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Xingyu Chen

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

INTRODUCTION

Concerns in the area of cybersecurity have recently been placed under the spotlight, particularly so when 2017 saw a substantial number of cyberattacks and security breaches across the world (Graham, 2017; Leech, 2017). The disruption and costs associated with cyber threats are also increasing exponentially over time, and have rendered such threats as one of the major concerns for many developed countries (Drzik, 2018; World Economic Forum, 2018).

When successful, the consequences of cyberattacks can be profound and manifold. At the individual level, for instance, confidential and sensitive data can be compromised, financial losses can occur, and essential operations can be disrupted (Accenture & Ponemon Institute LLC, 2017; Tham, 2017a). On the wider macro level, the malicious access into computer and network systems can compromise and cause the collapse of “critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population” (Lewis, 2002, p. 1). With the detrimental effects of cyberattacks, it is vital that these cyber threats are managed effectively, for which the present chapter will serve to shed light on the weakest player in the maintenance of cybersecurity – humans.

UNDERSTANDING THE WEAKEST LINK IN CYBERATTACKS: HUMAN BEHAVIOURS

Cyberattacks can be perpetuated via two means: (1) system-centric approach, where perpetrators exploit the technical vulnerabilities of a computer or network system to conduct an attack, and (2) user-centric approach, where negligence or mistakes of the computer users facilitated the execution of cyberattacks (Neupane, Rahman, Saxena, & Hirshfield, 2015). However, successful cyberattacks in reality are often a result of the latter, in which human errors rather than technological shortcomings are the main cause of concern (Kelly, 2017; Tasman-Jones, 2016). According to Symantec, 97 percent of malware attacks in 2016 targeted people and their poor online behaviours, with only the remaining three percent attributed to actual flaws in the network security system itself (Bennett, 2017).

DOI: 10.4018/978-1-5225-9715-5.ch065

Also known as social engineering, perpetrators commonly employ the method of “hacking humans” – rather than the system – by exploiting poor cyber behaviours to gain a backdoor in computer systems and networks (Choo et al., 2016). It encompasses deceiving and psychologically manipulating the victims into divulging confidential information, and/or getting them to perform certain actions that facilitate the execution of cyberattacks. For instance, the social engineering technique of “phishing” works because of the meticulously-crafted email messages that encourage recipients to click on the weblinks or download attachments that are malicious in nature (Lord, 2017; Tham 2017). In 2017, many ransomware attacks targeted at organisations had been caused by successful phishing attempts on unanticipating and careless employees, mainly through their emails or media (Jay, 2018).

Should one exercise caution, such phishing attempts may be avoided as poor human behaviour in the cyberspace forms the core of why many such cyberattacks are successful in the first place (Bennett, 2017; Fallows, 2011; Hadlington, 2017). As what Andy Waterhouse, EMEA Director at RSA Security (cited in Bennett, 2017, p. 12) had commented,

It is not just about silly errors but often a lack of training and understanding of the implications of clicking on a malicious link, going to a risky website or even setting up a service on a public cloud service without looking at the security implications.

The endeavour to combat one’s susceptibility to cyberattacks involve a long process of understanding the specific attributions that contribute to this susceptibility, as well as the necessary follow-up actions needed to be done to manage the threats. Approaches to mitigate the cyberattacks therefore goes beyond the protective capabilities of sophisticated technological solutions (Conteh & Schmick, 2016; Goldman, 2013), such as antivirus software and firewalls, and have to include human-centric measures.

UNDERSTANDING HUMAN-CENTRIC MEASURES

Importance of Good Cyber Hygiene to Manage Cyber Threats

Perpetrators are constantly searching for the weakest link in the computer or network system, in order to gain quick and easy but unauthorised access into these areas (Ashiq, 2015). Humans are unfortunately very much the weakest link in cybersecurity, because of their risky behaviours in the cyberspace (Vishwanath, 2016). A 2017 survey conducted by the Cyber Security Agency of Singapore (CSA), for instance, revealed that many people exhibit poor behaviours (e.g., using the same password for both personal and work accounts, not using two-factor authentication, not installing security on mobile phones, not running virus checks for files and devices before opening them) on online platforms that put themselves and their organisations at risk of cyberattacks (CSA, 2017b).

If poor human cyber behaviours are indeed the main cause of successful cyberattacks, then managing these behaviours should reduce one’s vulnerability towards cyberattacks. To do so, there is a need to reduce risky online behaviours as well as improve one’s cyber hygiene behaviours.

The Value of Cyber Hygiene Behaviours

Protective cyber behaviours are known as cyber hygiene behaviours. Just as how people brush their teeth and take showers to maintain their basic hygiene level and health, cyber hygiene practices are similar except that they take place in the cyberspace (Symantec Corporation, 2017). Cyber hygiene revolves around the implementation of cybersecurity ‘best practices’ to protect and maintain one’s online ‘safety’ and ‘health’ whilst using the computer and internet. It focuses on individual responsibility to perform the identified best practices, rather than depending on the technical protection measures against cyber threats (Aldoriso, 2018; Ashiq, 2015). Some examples of cyber hygiene practices include using an anti-virus software, activating firewalls, updating the operating system, wiping the hard drive, and using complex, unique passwords (Symantec Corporation, 2017).

The many years of effort to educate people on these protective measures¹ have seemingly produced limited results because people are generally still not engaging in adequate cyber hygiene practices. It becomes imperative to explore this phenomenon of non-action, and identify the what’s and why’s of not adhering to cyber hygiene practices despite the obvious value of these behaviours.

Awareness Does Not Equate to Frequency of Cyber Hygiene Practices

It is vital that people do not just know about cyber hygiene practices, but are also proactively undertaking such behaviours to protect themselves from cyber threats. The conventional understanding is that knowing how to and why one should engage in a certain behaviour should lead to the actual execution of the behaviour. However, awareness of cyber hygiene practices does not necessarily translate to its behavioural manifestation. People fail to follow cyber hygiene practices despite becoming increasingly aware about cybersecurity issues (Schick, 2018).

Understanding Poor Online Behaviours Based on Insights From Cyber Hygiene Surveys

Surveys conducted on the frequency of cyber hygiene practices of individuals across the world reveal similar trends. In the United States, the Ponemon Institute conducted a “The Cyber Hygiene Index: Measuring the Riskiest States” research and found that Americans display risky cyber habits (e.g., not downloading and using anti-virus software) despite being aware that they should not do so (Moffitt, 2018). Organisational employees were also engaging in risky behaviours (e.g., clicking on unverified links) despite fears of data breach, according to a survey by OpenVPN in America (Abel, 2018).

Findings from overseas surveys have been observed in Singapore as well. In a 2017 cyber hygiene survey² (CHS) conducted by the Home Team Behavioural Sciences Centre (HTBSC), results revealed that individuals tend to know why they should engage in good cyber habits and how to do them, but they are not really doing it³. With that, the 2017 CHS had also identified several cyber hygiene behaviours that people showed both high awareness of and high frequency in. This included checking the header of an incoming or new email, not clicking on hyperlinks from unknown senders, as well as using ad-block tools to block pop-ups.

Knowledge should stimulate constructive cyber behaviours, just as how education is needed to inform people the why’s and how’s of doing something. Yet, the discrepancy between awareness and frequency of cyber hygiene practices is worrying, because it highlighted underlying concerns that go beyond simply what education and information can do. The examination of motivations underlying this

phenomenon of non-action is henceforth critical, since it may contribute to efforts to improve individuals' cyber hygiene levels.

THERE ARE MANY PSYCHOLOGICAL REASONS FOR INACTION OF CYBER HYGIENE PRACTICES

The reasons for inaction of cyber hygiene practices cannot be attributed to a single factor. From a psychological perspective, various reasons can be identified to explain why people are not taking proactive steps to protect themselves from cyber threats, despite knowing the importance of doing so.

Lack of Individual Responsibility

The sense of individual responsibility can determine whether people will take necessary steps to protect themselves from cyberattacks. Responsibility is found to be related to action (Coleman, 2012), where people with a low sense of individual responsibility tend to be less motivated to engage in safe cyber hygiene practices.

In fact, cybersecurity research in organisational settings have demonstrated that people usually engage in these protective practices only if relevant social others are doing it (e.g., peers, colleagues, direct superiors), or simply if they are likely to get caught for not doing so (Herath & Rao, 2009). A 2016 survey conducted by HTBSC on 'Perceptions of National Resilience'⁴ further supported the notion of the lack of individual responsibility for dealing with cyberattacks. Far from seeing it as a responsibility that one should undertake, 64 percent of the respondents perceived that it is the government's duty instead to protect them from a cybersecurity crisis.

Low Cyber Risk Perception and Complacency

Optimism bias refers to the tendency for humans to underestimate the likelihood of negative events happening onto them (Sharot, 2011). In the context of cyber threats, it can result in a false sense of security, since individuals are likely to perceive themselves to be 'invulnerable' to attacks (Shah, 2014). Low cyber risk perception and complacency are likely to cause people to disregard cues of danger, behave recklessly online, and not take precautions to protect themselves from cyber threats.

The lack of experiences may further render individuals incognisant of how real the threat and consequences of cyberattacks are. Indeed, the absence of 'painful lessons' makes it difficult for one to justify why they should learn, engage in efforts, as well as mobilise valuable resources to build some degree of cyber defence (Siau, 2017). Furthermore, people may not necessarily engage in appropriate behaviours, unless they deem that the cyber threats will occur to them and that these threats are targeted at their personal concerns (Lee, Larose, & Rifon, 2008).

Lack of Usability Security

The implementation of cyber security measures will increase one's protection against cyber threats. However, it may also reduce the ease of use of technology (i.e., speed, convenience) and one's work productivity and efficiency on the device (Bruzzeze, 2015). This is also known as the lack of usability security. When people realise that they may experience reduced speed and convenience, they are less likely to engage in good cyber hygiene practices even if it means acquiring tougher security levels.

For instance, while a newer mobile phone operating system (OS) patch provides greater and more effective security measures, people may hesitate to update their OS if it slows down the processing speed of their phone. Additionally, if the process of updating the software of a computer is a slow endeavour and there are many computers that require updating, it could result in substantial opportunity costs between downtime and financial profits for the organisation. Consequently, the company may be tempted to forgo the benefits of the latest computer software update, and instead dedicate time to pursue financial earnings. Thus, whether or not individuals engage in cyber hygiene practices does depend on the consequences and their attitude towards it. If consequences are positive, a favourable attitude is likely to transpire, thereby increasing the likelihood that the cyber hygiene practice will materialise.

Difficulty in Learning and Implementing Good Cyber Hygiene Habits

The more technical a cyber hygiene practice is to perform, the less 'common sense' it becomes (Ng, 2017). The harsh truth is that if a cyber hygiene practice is perceived to be difficult to do, an individual naturally will be less likely to adopt that practice. For instance, checking if the secure sockets layer (SSL) is present is important before one conducts financial transaction via the internet. SSL refers to the lock icon beside the web address at the address bar of an internet browser, which is an indication as to whether a website is securely connected to the web server or not (GlobalSign, 2018). However, it can be a challenging thing to do if people are not aware of what exactly is SSL, or the steps needed to check the quality of the SSL certificate. Consequently, people may become less likely to check if the SSL is present and/or the quality of the SSL certificate.

On the opposite spectrum, cyber hygiene practices that are easy to execute and commit to are more likely to see a higher frequency of behavioural manifestation. This could be a potential reason for the high awareness and frequency of several behaviours, including the checking of email header and using ad-block tools to block pop-ups, since they do not require significant conscious effort to do so.

Lack of Others Who Are Also Engaging in Cyber Hygiene Practices

Normative beliefs focus on whether a person feels pressured to do something or not, based on what he or she observes others to be doing (Ajzen, 1991, 2002). In other words, individuals are likely to feel the need to engage in certain cyber practices simply because others are doing it. According to Herath and Rao (2009), the expectations and behaviours of relevant others, including superiors and peers, are significant influences on individuals' cyber security behaviours.

The awareness of why people engage or do not engage in certain cyber hygiene behaviours will be useful to inform and shape cybersecurity measures. People exhibit inaction for distinctive reasons, which perhaps then, lead to the requirement of a myriad of human-centric solutions, on top of technical security measures, to improve human cyber behaviours and reduce one's susceptibility to cyber threats.

IMPLICATIONS FOR DESIGNING HUMAN-CENTRIC APPROACH TO COMBAT CYBER THREATS

The reasons as to why people do or not do certain cyber hygiene practices differ from person to person, and even context to context. The development of measures to improve problematic cyber behaviours should henceforth be highly targeted and relevant, depending on the individuals' needs and the current climate of cyber threats. The following are some implications for designing human-centric measures against cyber threats.

Education on Cyber Threats Must Continue

Education is critical to help people understand why it is necessary for them to engage in good cyber habits. Consequently, it should prompt people to act to protect themselves from cyber threats, thereby reducing the inconsistency between people's awareness of cyber hygiene practices and how often they perform them. More importantly, besides informing people about the current climate of cyber threats, education should also include (i) how cyber perpetrators target victims (i.e., exploiting the lack of good cyber behaviours) as well as the common methods they use to execute their attacks (i.e., social engineering), and (ii) reasons that reduces the likelihood of practising these proper cyber practices so as to draw attention to this area of concern.

Regular mandatory cyber hygiene or cybersecurity programmes could be offered to people, such as the employees of an organisation or students from an educational institution. These trainings can serve as an effective platform to instil knowledge, address any misconceptions on cybersecurity issues, or for individuals to share and learn from one another on their experiences, if any, dealing with cyber threats. Participants do not have to be an actual victim before they can learn. The sharing and illustration of authentic experiences can aid internalisation of the seriousness of the cyber threat, whereby the fidelity of the victim's voice reinforces how real the threat and consequences are.

Tailor Outreach Messages

Various sources of information can be condensed into digestible bite-sized knowledge and contribute to educational material. Local and international cyber threats can be studied holistically to identify new or emerging trends. Primary data may also be gathered to contribute to teaching resources, including interviews with incarcerated attackers to understand common modus operandi and the human vulnerabilities they target to facilitate their attacks.

Outreach messages ideally should be tailored to different societal groups, according to various demographic markers such as age – i.e., the types of cyber threats affecting the young and the old may differ, dictating the need to introduce tailored measures. Furthermore, targeted messages may help particular groups to understand and better relate to the current climate of cybersecurity using appropriate case examples and interventions. When the target audience understands why cybersecurity is an issue for them, it becomes easier for them to change their attitudes. Constant reminders are necessary as well, since people are likely to forget and become complacent over time. Different modes of transmitting these messages can be utilised. For people who particularly do not have sufficient time to read their emails or cyber security advisories, sending concise email reminders on the importance of practicing good cyber habits is a feasible alternative.

There is also the need to revise educational messages occasionally, in order to recapture people's attention over time (Belch & Belch, 2009). An underlying reason for doing so arises from the concern that constant exposure to the same messages can ultimately result in individuals being desensitised – or numb – towards these messages (So, Kim, & Cohen, 2017).

The Need to Nudge Humans to Engage in Cyber Hygiene Practices

Education by itself is clearly not sufficient. This was seen in the 2017 CHS results, in which people are still not engaging in important cyber actions despite knowing why or how they should do it. This highlighted underlying issues that goes beyond what education can do.

The nudge theory can be employed to complement outreach efforts. A nudge prompts people to take action by subtly making the decision-making process easier (Chu, 2017). The decisions that an individual have to make, or the thought processes that they have to undergo first, can be complicated enough such that it prevents or slows down the occurrence of engaging in good cyber behaviours altogether. Automation, for instance, is a nudging method whereby people are automatically required to do something unless they opt-out of it (if there is an opportunity to do so). In the context of cyber hygiene practices, this could mean setting various practices as a default feature or behaviour (i.e., natural 'opt-in') that people have to engage in when they use the computer or internet. As a result, it removes the need for people to proactively undertake constructive cyber practices. Higher participation and compliance to regulations are consequently more likely to follow as well (Blau, 2017).

Automation can also make certain practices less difficult or tedious to do (e.g., reduces the amount of time, effort, and knowledge needed to perform it), thereby increasing the likelihood that people will eventually engage in these protective measures.. When barriers to action (e.g., technical details) are removed, a certain action becomes easier to carry out.

Conduct Red-Teaming Exercises

The objective of red-teaming exercises is to “obtain a realistic level of risk and vulnerabilities against your technology, people and physical/facilities” (RedTeam Security Consulting, 2016, p. 1). One method to do so is to invite white hats to hack into these systems, therefore checking the resiliency of an organisation's computer and network systems. In other words, a cyberattack will be purposefully – with no malicious intention – conducted without employees' knowledge of the exercise, to reveal the ways in which cyber perpetrators can exploit to enter the organisation's computer and network systems. This includes identifying both human and technical vulnerabilities.

The benefit of red-teaming also lies in its capacity to create a level of psychological fidelity, allowing people to experience the effects of a real cyberattack but under safe circumstances with minimal repercussions. According to Boud, Cohen, and Walker (1993), such experiences can help to accentuate the criticality of cyber issues within the organisation. With red-teaming exercises, it is with the expectation and hope that people will be more careful and thus practice good cyber hygiene practices in the future, after experiencing the negative emotions and consequences of a cyberattack.

Nonetheless, there is a need to balance between the endeavour of identifying the vulnerabilities of one's online security system and the potential negative emotional exerted on the “victims” as a result of such exercises. Should red-teaming exercises be conducted, there is a need to provide debriefs to these individuals to help manage their reactions.

Regulations to Ensure Compliance to Cyber Hygiene Practices

Certain cyber threats lay dormant and are not obvious unless a computer or network system is consciously scanned for compromise. Unfortunately, the notion of reviewing these systems on a regular basis may not be welcomed, particularly when the process is time-consuming and effortful. Regulations to drive for consistent audits should hence be implemented. These regulations may also include policies to ensure that people are mandated to engage in other necessary cyber hygiene practices.

Furthermore, detection mechanisms to detect lack of compliance could be developed and executed alongside these regulations. As expressed by Herath and Rao (2009), people will observe rules simply because of the fear of being discovered to be not observing them. To ensure its effectiveness, such detection mechanisms initiatives should be clearly communicated to the employees in advance, and constantly reinforced. A subtler option to get people to start complying with cyber hygiene practices is ensuring that superiors or leaders in an organisation are doing so as well, since people are likely to model after significant others who are deemed to be important characters within the organisation. In the long-run, this may create a culture in the organisation that engaging in good cyber hygiene is common and normal, and that compliance to cybersecurity protocols is indeed necessary.

CONCLUSION

Understanding the nature of human behaviours on the cyber space is critical, given that poor cyber practices on this platform has clearly led to the successful execution of cyber threats. Poor human behaviours of varying kinds offer perpetrators the window to exploit these vulnerabilities to facilitate their attacks, and plenty can be done to help humans engage in better online hygiene practices.

Nonetheless, much more research still needs to be conducted in this area, given its emerging yet imperative nature. More comprehensive studies looking at the relationships between online human behaviours and cyberattacks – or even the modus operandi of perpetrators – will indefinitely be useful. This can shed light on what exactly is critical and needs to be worked on.

It remains clear at the end of the day, that technological vulnerabilities is only just one small reason why cyber threats have proliferated and blossomed today. The role of poor human cyber behaviours cannot be ignored or undermined, because they are a, if not one of the more important, cause of concern.

REFERENCES

Abel, R. (2018, June 18). Despite advancements, employees still practice bad cyber-hygiene, study. *SC Media*. Retrieved from <https://www.scmagazineuk.com/despite-advancements-employees-practice-bad-cyber-hygiene-study/article/1486713>

Accenture and Ponemon Insitute. (2017). *2017 cost of cyber crime study: Insights on the security investments that make a difference*. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Aldoriso, J. (2018, March 26). What is cyber hygiene? A definition of cyber hygiene, benefits, best practices, and more. *Digital Guardian*. Retrieved from <https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>

Ashiq, J. (2015, April 30). The Importance of cyber hygiene in cyberspace. *Infosec Institute*. Retrieved from <http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace/#gref>

Belch, G. E., & Belch, M. A. (2009). Source, message, and channel factors. In *Advertising & promotion: An integrated marketing communications perspective* (8th ed.; pp. 174–205). Boston: McGraw-Hill Irwin.

Bennett, M. (2017). Building a digital security army. *The Telegraph*. Retrieved from <https://www.telegraph.co.uk/business/digital-security/human-behaviour-in-digital-security/>

Blau, A. (2017, December 11). Better cybersecurity starts with fixing your employees' bad habits. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits>

Boud, D., Cohen, R., & Walker, D. (1993). Using experience for learning. Bristol, PA: The Editors and Contributors.

Choo, B., Dillon, L., Neo, L. S., Ong, G., Tan, E., & Khader, M. (2016). *Social engineering: Using psychology to exploit bugs in the human operation system (HTBSC Research Report No.: 01/2016)*. Singapore: Ministry of Home Affairs, Home Team Behavioural Sciences Centre.

Chu, B. (2017, October 9). What is 'nudge theory' and why should we care? Explaining Richard Thaler's Nobel economics prize-winning concept. *Independent*. Retrieved from <https://www.independent.co.uk/news/business/analysis-and-features/nudge-theory-richard-thaler-meaning-explanation-what-is-it-nobel-economics-prize-winner-2017-a7990461.html>

Coleman, J. (2012, August 30). Take ownership of your actions by taking responsibility. *Harvard Business Review*. Retrieved from <https://hbr.org/2012/08/take-ownership-of-your-actions>

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31–38. doi:10.19101/IJACR.2016.623006

CSA. (2017a, February 10). *CSA launches First National Cybersecurity Awareness Campaign*. Retrieved from https://www.gov.sg/~sgpcmedia/media_releases/csa/press_release/P-20170210-1/attachment/CSA%20Launches%20First%20National%20Cybersecurity%20Awareness%20Campaign_10%20Feb%202017.pdf

CSA. (2017b, February 15). *CSA releases key findings from first Cybersecurity Public Awareness Survey*. Retrieved from http://www.nas.gov.sg/archivesonline/data/pdfdoc/20170215003/140217_CSA%20Releases%20key%20findings%20from%20first%20cybersecurity%20public%20awareness%20survey.pdf

Curtin Singapore's website defaced by hackers claiming to represent ISIS. (2015, March 10). *Today*. Retrieved from <https://www.todayonline.com/singapore/curtin-singapores-website-defaced-hackers-claiming-represent-isis>

Cyber Aware. (n.d.). Retrieved from <https://www.cyberaware.gov.uk>

Cyber Security Campaign. (n.d.). Retrieved from <https://www.cybersecuritycampaign.com.hk/index-en.html#>

Drzik, J. (2018, January 17). Cyber risk is a growing challenge. So how can we prepare? *World Economic Forum*. Retrieved from <https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready>

Fallows, J. (2011, March 24). Cyber-security can't ignore human behaviour. *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2011/03/cyber-security-cant-ignore-human-behavior/72826/>

Foo, S., & Jayakumar, S. (2018, January 26). Cyber threats: 2018 and beyond. *The Straits Times: Opinion*. Retrieved from <https://www.straitstimes.com/opinion/cyber-threats-2018-and-beyond>

Get Safe Online. (2018). Retrieved from <https://www.getsafeonline.org>

GlobalSign. (2018). *What is SSL?* Retrieved from <https://www.globalsign.com/en-sg/ssl-information-center/what-is-ssl/>

Goldman, D. (2013, January 31). Your antivirus software probably won't prevent a cyberattack. *CNN Tech*. Retrieved from <https://money.cnn.com/2013/01/31/technology/security/antivirus/index.html>

Graham, L. (2017, September 20). The number of devastating cyberattacks is surging – and it's likely to get much worse. *CNBC*. Retrieved from <https://www.cnn.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html>

Greig, J. (2018, April 19). Why human vulnerabilities are more dangerous to your business than software flaws. *TechRepublic*. Retrieved from <https://www.techrepublic.com/article/why-human-vulnerabilities-are-more-dangerous-to-your-business-than-software-flaws/>

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon (London)*, 3(7), e00346. doi:10.1016/j.heliyon.2017.e00346 PMID:28725870

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. doi:10.1057/ejis.2009.6

Iswaran, S. (2018, August 6). Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity, on the cyber-attack on SingHealth's IT system, during Parliamentary Sitting, 6 August 2018. *Ministry of Communications and Information*. Retrieved from <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/8/statement-by-mr-s-iswaran-on--cyber-attack-on-singhealth-it-system-during-parl-sitting-on-6-aug-2018>

Jay, J. (2018, March 31). Hackers still exploiting the human factor to carry out ransomware attacks. *SC Media*. Retrieved from <https://www.scmagazineuk.com/hackers-exploiting-human-factor-carry-ransomware-attacks/article/1472956>

Kelly, R. (2017, March 3). Almost 90% of cyber attacks are caused by human error or behaviour. *Chief Executive*. Retrieved from <https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/>

Kwang, K. (2018, July 20). Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted. *Channel NewsAsia*. Retrieved from <https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318>

- Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445–454. doi:10.1080/01449290600879344
- Leech, M. (2017, September 21). Data breach statistics 2017: First half results are in. *Gemalto*. Retrieved from <https://blog.gemalto.com/security/2017/09/21/new-breach-level-index-findings-for-first-half-of-2017/>
- Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic and International Studies.
- Lim, J. (2013, October 30). Ang Mo Kio Town Council website hacked. *The Straits Times*. Retrieved from <https://www.straitstimes.com/singapore/courts-crime/ang-mo-kio-town-council-website-hacked>
- Loke, K. F. (2017, February 28). MINDEF Internet system breached; data stolen from national service-men, employees. *Channel NewsAsia*. Retrieved from <http://www.channelnewsasia.com/news/singapore/mindef-internet-system-breached-data-stolen-from-national-servic-7617146>
- Lord, N. (2017, July 27). What is a phishing attack? Defining and identifying different types of phishing attacks. *Digital Guardian*. Retrieved from <https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks>
- Moffitt, T. (2018, June 5). American cybercrime: The riskiest states in 2018. *Webroot: Smarter Cybersecurity*. Retrieved from <https://www.webroot.com/blog/2018/06/05/2018-riskiest-states-for-cybercrime-in-america/>
- Mokhtar, F. (2018, June 19). Cyber threats in Singapore go up; phishing attacks see biggest jump. *Today*. Retrieved from <https://www.todayonline.com/singapore/cyber-threats-singapore-go-phishing-attacks-see-biggest-jump>
- No Internet access for public officers' work computers by next June. (2016, June 8). *Channel NewsAsia*. Retrieved from <https://www.channelnewsasia.com/news/singapore/no-internet-access-for-public-officers-work-computers-by-next-ju-7961140>
- PwC. (2016a). Adjusting the lens on economic crime. *Global Economic Crime Survey 2016*. Retrieved from <https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf>
- PwC. (2016b). *PwC's 2016 Global Economic Crime Survey – Singapore*. Retrieved from https://www.pwc.com/sg/en/consulting/assets/economic-crime-survey/economic_crime_survey_2016_singapore.pdf
- PwC. (2017). *Global State of Information Security Survey 2017: Singapore highlights*. Retrieved from <https://www.pwc.com/sg/en/risk-assurance/assets/gsis/global-state-of-information-security-survey-2017-sg.pdf>
- RedTeam Security Consulting. (2016). *Full Force Red Team*. Retrieved from <https://www.redteamsecure.com/red-teaming/>
- Schick, S. (2018, June 13). Poor password practices put corporate cybersecurity at risk. *Security Intelligence*. Retrieved from <https://securityintelligence.com/news/poor-password-practices-put-corporate-cybersecurity-at-risk/>

Shiao, V. (2017, August 1). A third of Singapore SMEs hit by ransomware last year: study. *The Business Times*. Retrieved from <https://www.businesstimes.com.sg/technology/a-third-of-singapore-smes-hit-by-ransomware-last-year-study>

Singtel. (2018, May). *Managing cyber security incidents before they become crises*. Retrieved from <https://www.singtel.com/business/singtel-global-services/content/managing-cyber-security-incidents-before-they-become-crises>

So, J., Kim, S., & Cohen, H. (2017). Message fatigue: Conceptual definition, operationalization, and correlates. *Communication Monographs*, 84(1), 5–29. doi:10.1080/03637751.2016.1250429

Strategy for a Technology-driven Future. (2017, November 3). *Infocomm Media Development Authority*. Retrieved from <https://www.imda.gov.sg/infocomm-and-media-news/buzz-central/2016/6/strategy-for-a-technology-driven-future>

Symantec Corporation. (2017). Good cyber hygiene. *Norton by Symantec*. Retrieved from <https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html>

Tasman-Jones, J. (2016, March 31). Human behaviour still biggest cause of cybercrime. *Fund Strategy*. Retrieved from <https://www.fundstrategy.co.uk/human-behaviour-still-biggest-cause-of-cybercrime/>

Tham, I. (2017a, May 12). Hackers broke into NUS, NTU networks in search of government, research data. *The Straits Times*. Retrieved from <http://www.straitstimes.com/singapore/hackers-broke-into-nus-ntu-networks-in-search-of-government-research-data>

Tham, I. (2017b, May 21). Cyber hackers and digital defences: Gone phishing... So, everyone, on guard. *The Straits Times*. Retrieved from <http://www.straitstimes.com/tech/gone-phishing-so-everyone-on-guard>

Tham, I. (2017c, September 7). AXA data breach affects 5,400 Singapore customers. *The Straits Times*. Retrieved from <http://www.straitstimes.com/singapore/axa-data-breach-affects-5400-singapore-customers>

Tham, I. (2018). Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack. *The Straits Times*. Retrieved from <https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most>

Vishwanath, A. (2016, May 5). Cybersecurity's weakest link: humans. *The Conversation*. Retrieved from <https://theconversation.com/cybersecuritys-weakest-link-humans-57455>

World Economic Forum. (2018). *The Global Risks Report 2018*. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

ADDITIONAL READING

Blau, A. (2017, December 11). Better cybersecurity starts with fixing your employees' bad habits. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits>

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31–38. doi:10.19101/IJACR.2016.623006

Foo, S., & Jayakumar, S. (2018, January 26). Cyber threats: 2018 and beyond. *The Straits Times: Opinion*. Retrieved from <https://www.straitstimes.com/opinion/cyber-threats-2018-and-beyond>

Goldman, D. (2013, January 31). Your antivirus software probably won't prevent a cyberattack. *CNN tech*. Retrieved from <https://money.cnn.com/2013/01/31/technology/security/antivirus/index.html>

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. doi:10.1057/ejis.2009.6

Iswaran, S. (2018, August 6). Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity, on the cyber-attack on SingHealth's IT system, during Parliamentary Sitting, 6 August 2018. *Ministry of Communications and Information*. Retrieved from <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/8/statement-by-mr-s-iswaran-on--cyber-attack-on-singhealth-it-system-during-parl-sitting-on-6-aug-2018>

Vishwanath, A. (2016, May 5). Cybersecurity's weakest link: humans. *The Conversation*. Retrieved from <https://theconversation.com/cybersecuritys-weakest-link-humans-57455>

World Economic Forum. (2018). *The Global Risks Report 2018* [PDF document]. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

KEY TERMS AND DEFINITIONS

Cyber Hygiene: Cyber protective behaviours that people engage in whilst on the computer and internet, such as installing and updating anti-virus software.

Cyberattack: A form of cyber threat whereby perpetrators aim to create a backdoor in a computer or network system to gain unauthorised access into these systems.

Optimism Bias: A human tendency where people overestimate the likelihood of good things and underestimate the likelihood of bad things happening onto them.

Social Engineering: The psychological manipulation of victims by cyber perpetrators, in order to get victims to divulge sensitive confidential information, or to perform certain actions that help perpetrators to successfully execute their cyberattacks.

ENDNOTES

¹ Such as Singapore's First National Cybersecurity Awareness Campaign launched by CSA in early 2017 (CSA, 2017a), United Kingdom's GetSafeOnline Campaign (Get Safe Online, 2018) and Cyber Aware Campaign (Cyber Aware, n.d.), as well as Cyber Security Campaign in Hong Kong (Cyber Security Campaign, n.d.).

² In collaboration with social engineering expert Dr Arun Vishwanath from the Department of Communication in University at Buffalo, HTBSC conducted a survey that assesses for various facets of Singaporeans' cyber hygiene. In particular, it assesses for: (1) awareness of cyber hygiene practices, (2) frequency of cyber hygiene practices (a total of 39 different practices were assessed), (3) risk beliefs, (4) phishing knowledge, and (4) reporting behaviour. A total of 404 responses were

collected from the community (using convenience sampling method), with respondents from age 16 to 67 years old.

- ³ According to the CHS, some top problematic cyber hygiene practices (in which people know why and how they should do it), are (in no sequence): using incognito mode or private mode when routinely surfing the internet, create new/unique logins and passwords for all online sign-ins, using a VPN when in an open/public Wi-Fi network, clearing browser cache, creating complex logins and passwords, checking device to ensure that it has the latest OS, software update, or patch, clearing cookies on browser, changing default passwords on all Internet-enabled devices, managing how browser stores passwords, storing logins and passwords on encrypted online password vaults, managing privacy settings on social media platforms, keep virus protection updated, running a virus scan on any new USB or external storage device.
- ⁴ A segment of the 'Perceptions of National Resilience' survey assesses individuals' perceptions of how likely various crisis scenarios will happen in Singapore, and to what extent are individuals, community, and government responsible for responding to crisis scenarios such as cybersecurity crisis. A representative total of 3000 Singaporeans' responses was collected.

Understanding the Relationship Between Cybercrime and Human Behavior Through Criminological Theories and Social Networking Sites

Anne-Marie Mohammed

The University of the West Indies, St. Augustine, Trinidad and Tobago

Vladlena Benson

Aston Business School, UK

George Saridakis

University of Kent, UK

INTRODUCTION

Social networking sites (SNS) are, “applications that enable users to connect by creating personal information profiles, inviting friends and colleagues to have access to those profiles, and sending e-mails and instant messages between each other” (Kaplan and Haenlein, 2010:63). Any type of information such as blogs, photos, videos and audio files can exist within these personal information profiles. Therefore, SNS can be viewed as virtual communities that enable on-demand communication and interaction with real-life friends as well as the ability to meet new friends from around the world based on similar interest (Kuss and Griffiths, 2011). The rapid growth in usage of SNS worldwide in recent years, permits its description as a ‘global consumer phenomenon’ (Kuss and Griffiths, 2011). While there are great advantages for the use of SNS, one research by Kuss and Griffiths (2017) suggests that constant usage can create the perception of a need to be online. This may result in compulsive and excessive use of SNS and in some cases give rise to symptoms associated with substance-related addiction. This excessive use of SNS can reduce the productivity of users as well as increase their exposure to cyberattacks. On the other hand, a recent study by Allcott et al. (2019), explores the welfare effects of SNS and discovers that the majority of their sample value access to SNS for four weeks is at US \$100 or more. Therefore, this valuation suggests that consumer surplus for SNS is expected to be in the billions of dollars considering the large number of active users globally. According to Pew Research Center (2018), Facebook and YouTube are the most popular SNS among adults whereas Snapchat and Instagram are the most popular among young adults. Facebook is by far the most popular social networking site globally with 1.52 billion active daily users and 2.32 billion active monthly users (Facebook, 2018).

SNS have become the mainstream communication medium for individuals, especially young people (Holt and Bossler, 2014), and businesses (Culnan et al., 2010). At present there are approximately 4.17 billion internet users worldwide, thus demonstrating a sustained growth from the year 2015 by a quarter. Of these, 3.4 billion are active social media users with a similar proportion of mobile internet users (3.7 billion) according to Statista (2018). However, with the continuous loss of control over personal information that is exposed online, individuals and businesses present easy targets for non-technical attacks

DOI: 10.4018/978-1-5225-9715-5.ch066

ranging from spear-fishing to whaling leading to serious cyber victimization (McAlaney et al., 2018). Cybersecurity professionals agree that this security depends on people more than on technical controls and countermeasures. Recent reviews of cyber security express that no industry sector is invulnerable to cyber-attacks and that the public sector tops the list for targeted security incidents (Benson, 2017). This is largely attributed to the weaker cyber security mind-set of employees. On the other hand, the financial sector, year on year, experiences the highest volume of cyber breaches. These are predominantly aimed at financial gain or espionage. What is common among these rather different sectors is that the attack vector by cyber criminals starts with social engineering. The weakest link in the security chain is still the human element. Irrespective of the market segment, the losses contributing to the current global cost of cybercrime are huge with an estimation of approximately \$600 billion (McAfee, 2018).

Unsurprisingly, the human behavior in an online context has been addressed by researchers for some time. The cybersecurity industry, policymakers, law enforcement agencies and public as well as private sector organizations are yet to realize the factors affecting the risk of online victimization and the impact on individuals and businesses (Taylor et al., 2010). In order to improve cybersecurity practices, there is a need for a discussion acknowledging that cybersecurity is inherently a complex socio-technical system.

This chapter presents an overview of emerging issues in the psychology of human behavior and the evolving nature of cyber threats. Theories of crime and empirical studies on user victimization as seen on social networks are reviewed. The chapter reflects on the role of social engineering as the entry point of many sophisticated attacks and highlights the relevance of the human element as the starting point of implementing cyber security programs in organizations as well as securing individual online behavior. There are numerous theories of crime that are relevant and applicable to cybercrime. However, this chapter focuses specifically on the routine activity theory (RAT) put forward by Cohen and Felson (1979) and the general theory of crime (GTC) introduced by Gottfredson and Hirschi (1990). These have relevance since the GTC is the most eminent latent trait theory of crime (Siegel, 2006) and the RAT gives a sociological explanation aimed at crime events rather than criminal propensities (Schaefer and Mazerolle, 2017), thus making both theories interesting and suitably applicable to cybercrime. This chapter also mentions the rational choice theory (RCT) as well as the deviant place theory (DPT) but to a lesser extent simply touches on some of the other existing theories of crime. For example, Cohen and Felson (1979) argue that crime will occur when there is a motivated offender, a suitable target/potential victim and the absence of guardians capable of preventing any violation. The latter can be in the form of physical guardianship (e.g. antivirus) or personal guardianship (e.g. computer skills). In addition, Gottfredson and Hirschi (1990) suggest that crime and victimization are associated with low levels of self-control. We then turn to empirical studies that have examined the user behavior on SNS leading to victimization (e.g. Hansen et al., 2017; Saridakis et al., 2016; Benson et al., 2015a-c). Issues associated with the emerging trends in human behavior research and ethics are presented for further discussion. The chapter concludes with a set of open research questions warranting immediate academic attention to avoid the exponential growth of future information breaches.

BACKGROUND: THEORIES OF CRIME

Research suggests that the frequency of internet usage shares a positive association with cyberbullying and victimization (Mesch, 2009). However, in modern times, most individuals, public organizations and private ones are heavily dependent on the usage of the internet to carry out their daily business activities and communications, therefore, limiting internet use is not a plausible solution to the problem of being

a victim of cybercrime. Thus, there is a need for examining the roots of the problem, which starts with people and the psychology behind human behavior that triggers cybercriminal activities. To this end, a number of theories have been developed to explain the psychology behind criminal activities. The RAT proposed by Cohen and Felson (1979), for example, suggests that crime is contingent on the following three components: exposure to a motivated offender, a suitable target and the lack or absence of capable guardians to prevent the violations. Furthermore, Cohen and Felson (1979) describe the suitability of a target as their attractiveness to the motivated offender as well as their availability for the crime. Therefore, if there is a situation where all three components of the RAT are present, then a crime is likely to occur.

According to Marcum et al. (2010), crime is not a random event, instead it follows a consistent pattern where the three components of the RAT are required. Eck and Clarke (2003) propose that the RAT can be expanded for cybercrimes where the offender and target do not necessarily share the same physical space but can share the same cyberspace such as the internet or any shared network.

In the context of cybercrime, the motivated offender is someone who is not only capable of committing the cybercrime but is also willing to commit it because he/she is motivated by personal gain such as identity theft, phishing, espionage, unfair investment information, bank fraud, someone's personal information or even revenge. The suitable target can be an individual or an organization who possesses the online information from which the motivated offender can gain. Finally, the guardian can be in the form of a software guardianship (e.g. antivirus or firewall), personal guardianship (e.g. computer skills or cybercrime awareness) and even physical guardianship such as a capable cybercrime unit or security personnel who can protect the parameters of an organization from intruders seeking to gain access to their network server.

Marcum et al. (2010) derive an explanation for the online victimization of youths (generation Z) using the RAT by suggesting that the great length of time spent on SNS increases their exposure to a motivated offender. Also, the types of information that they provide on these SNS (i.e., age, relationship status, daily activities, and pictures) make them suitable targets for online victimization. Furthermore, the insecure location in which the internet is being used by youths combined with their personal and parents' lack of expertise in cyber technology or internet security provides the third component of the RAT, which is the lack of capable guardianship.

While we reason that prior experience of online victimization by individuals on SNS increases their probability of noticing online security features and increasing their guardianship, a study by Benson et al. (2015b) finds otherwise. Benson et al. (2015b) find that there is no connection between these two factors and suggest that this can be explained through an individual's perception of the utility obtained from SNS for entertainment, socializing and other activities which is higher than the risk of online victimization to them.

Another major theory that is used to explain crime and victimization is the GTC, proposed by Gottfredson and Hirschi (1990) which suggests that the principal causal agent of all crimes and victimization is low self-control. There are six elements associated with low levels of self-control, which are: lack of future orientation, temper/anger, lack of diligence, self-centeredness, preference for risk taking and a preference for physical over mental tasks (Piquero et al., 2005). Individuals with low self-control are more likely to get angered easily than their counterparts who have high self-control and a similar statement can be made about each of the six elements associated with low self-control. According to Gottfredson and Hirschi (1990) there is a lot of shared personal and social characteristics between victims and offenders. Piquero et al. (2005) suggest that offenders of crimes are more likely to be victims of crime compared to non-offenders. The six elements of low self-control can be used to explain cybercrime offenders and cybercrime victimizations.

Individuals who demonstrate the first element, which is a lack future orientation, can influence victimization because they do not consider the long-term consequences of their actions neither do they take precautionary measures to protect the image of their online identities nor to protect their private and personal information from being stolen and shared on the internet. On the other hand, offenders of cybercrime demonstrate a lack of future orientation by failing to consider the illegality of the cybercrimes which they are committing and the long-term consequences if caught, which can possibly include jail sentences and permanent criminal records.

The second element, anger/temper, can result in individuals expressing these emotions on SNS which may include politics and other topics that can potentially elicit counter-controlling responses by other individuals who may be offended and thus respond through a cyber-bullying attack. Some cybercrimes such as cyber-bullying and cyber-harassment are as a result of offenders who hold anger for other individuals or firms and therefore seek revenge through cyberattacks.

The third element, lack of diligence, can increase victimization since an individual who lacks tenacity is less likely to take precautionary measures against cyberattacks such as the installation of an antivirus or firewall and the assurance that it is updated regularly.

Offenders who engage in cybercrimes such as phishing, espionage, bank fraud and the theft of personal information for financial gain exhibit a lack of diligence by choosing to commit cybercrime in order to generate income instead of a legal job. The fourth element, self-centeredness, relates to victimization. Since self-centered individuals are more likely to ignore the advice or request of others and show concern only for their own situation, this can create a lack of awareness of current cybercrime activities and preventative measures. Offenders demonstrate self-centeredness through their lack of care for their victims' emotional trauma or financial struggle that can arise from cybercrimes. The fifth element, preference for risk taking, increases victimization since individuals who are risk takers may visit more risky websites, purchase at untrusted retailers for lower prices and even skip security checks, thus increasing their probability of being attacked. Offenders of cybercrime are also risk takers since the act of committing these crimes exposes them to the consequential risk of being caught. The final element of low self-control can influence victimization since in non-cybercrimes we can argue that individuals who prefer physical tasks over mental ones are more likely to respond physically when faced with a hostile situation rather than use cognitive skills to arrive at a solution which is similar for offenders. This final element of low self-control is the only one that may not support cybercrime since the offenders of this must have the mental capacity required to commit such an act. According to Schreck (1999) vulnerability to victimization is a by-product of the psychological appearances of low self-control.

Another theory that describes the psychology of human behavioral influence on crime is known as the RCT. This theory explains that an offender will violate the law after rationally considering personal factors (i.e., the need for money, family, dependents, revenge, consequence and entertainment) and situational factors (i.e., how well the target is guarded and the competence of the local police service). Therefore, if an offender rationalizes that the consequential risk of the crime does not outweigh the reward gained from committing this crime, then the offender will commit the crime (Siegel, 2006). In the context of cybercrime, an offender will commit an act such as cyber-bullying, cyber-harassment, identity theft, espionage and even theft of personal and banking information if the satisfaction obtained through committing any of these cybercrimes is greater than the probability of getting caught by officials in addition to the dissatisfaction felt as a result of the consequences. The RCT can explain how the high number of cybercrimes worldwide, due to the low probability of being caught, may be because of a lack of efficiency, competence and training of local police officials in handling cybercrime incidents. There

exist very few studies which used the RCT to explain cybercrime activities, therefore more research is needed in this area.

Finally, there also exists the DPT that is used to explain victimization. According to this theory, individuals who have higher exposure to dangerous places have a higher probability of being a victim of a crime (Siegel, 2006). Therefore, this theory suggests that individuals should avoid dangerous places (e.g. crime hotspots) to lower their probability of being victimized. This theory can be expanded to include cyberspace and not just a physical space. Therefore, in the context of cybercrime, individuals who are exposed to dangerous cyberspace such as unsecure websites and unsecure internet networks, are more likely to be victims of a cybercrime. This theory is closely related to the RAT since the exposure to a dangerous place used in the DPT is similar to the concept of the convergence of the motivated offender and a suitable target used in the RAT.

FOCUS OF THE ARTICLE: LINKING CRIME THEORIES AND EMPIRICAL EVIDENCE

Cyber threats lead to two types of crimes (McAlaney et al., 2018) namely cyber-enabled and cyber-dependent crimes. On one hand, the internet technology is used to assist existing offences and such cyber-enabled crimes include e.g. fraud. The first vector of attacks is often established through the social media, where the offender researches the victims' profiles and/or gets in touch with them. Therefore social media serves as an assistive technology to cyber-enabled crimes. On the other hand, cyber-dependent crimes exist owing to the opportunities offered by the internet technology. Both hacking and malware distribution are examples of cyber-enabled crimes. These crimes are often perpetrated and spread via social platforms, thus making social network enablers of convergence of the motivated offender and a suitable target (Saridakis et al., 2016).

There are numerous studies worldwide that have adopted some of these theories of criminology to address the issues surrounding crime, and these theories have been expanded to be used in the analysis of cybercrime in recent times. One such example is a study by James et al. (2014) which suggests that older individuals are more likely to be targets for cybercrimes due to accumulated wealth, social unfamiliarity and trusting nature. This is consistent with the RAT since the older an individual is, the more suitable a target he/she becomes for a motivated offender due to the lack of guardianship. More young adults use the internet and more frequently than older adults, in fact 89% of young adults between the ages of 18-29 uses the internet for social media (Pew Research, 2015). This age group is very similar to the age group of university students. This group also manifests the preferences for conducting the commercial and business activities in purely online mode, making themselves the prime targets for criminal activities within cyberspace. A study by Benson et al. (2015c) finds that university students are less likely to be victims of cybercrimes as compared to non-university students. This can be explained using the Gottfredson and Hirschi (1990) GTC, since university students are generally more future oriented and thus have a higher level of self-control as compared to non-university students. Alternatively, this can also be explained using the RAT since internet servers used by universities are very secure and therefore increase the guardianship to prevent cybercrimes.

Research by Marcum et al. (2010) shows that a higher exposure to motivated offenders combined with allowing personal information to be accessible online, results in a higher probability of online victimization among college and high school students. Furthermore, a study done by Marcum et al. (2010) shows that communication with strangers online and provision of online contacts with personal or private

information are the most significant predictors of cyber victimization. This study is consistent with the RAT and since this activity merges the motivated offender with the suitable target, it is also consistent with the GTC as sharing of private information with strangers is a risky activity associated with lower levels of self-control. Also, it is consistent with the DPT since spending time on social networks with strangers increases your exposure to victimization in a dangerous place (cyberspace).

The RAT describes the importance of guardianship in the fight against crime and as a preventative measure against victimization. One form of guardianship in the context of cyberspace is security software. However, the UK Government's National Cyber Security Tracker revealed that only 44 percent of the internet users in the UK installed a security system such as an antivirus software, 37 percent updated these software regularly and furthermore, only 57 percent ensured that a website was secure before purchasing from that website (Home Office 2013, as cited in Williams, 2015). Williams (2015) finds that there is a negative relationship between software guardianship (e.g. antivirus and firewall) and identity theft victimization and his research quantifies this negative relationship by saying that a reduction in software guardianship by one point will result in an increase in identity theft victimization by 1.32 times. Additionally, a study on child online safety by Tennakoon et al. (2018) finds that self-employed parents are more likely to monitor their children's internet activities compared to parents who work in the private sector. Hill and Duncan (1987) suggest the "absent mother" hypothesis, which argues that when a mother works away from home it affects her child's behavior and development since her ability to supervise and socialize with her child is restricted and limited. McLanahan (1985) propose a similar explanation for absent fathers. Therefore, self-employed parents provide extra guardianship through monitoring of their children's internet usage, which explains the increased guardianship that would result in a lower risk of children being victims of cybercrimes, according to the RAT. Furthermore, Tennakoon et al. (2018) find that self-employed parents use online technology more frequently and are more aware of possible threats online such as cybercrimes, therefore this increases their capabilities as guardians to protect their children from cyberattacks.

Cybercrime includes identity theft and online banking information fraud. A study by Williams (2015) finds that individuals who sell goods online have a victimization rate that is 1.56 times higher than those who do not sell goods online. Another study by Pratt et al. (2010) finds that the routine of online shopping at online stores and spending time online are significant predictors of cybercrime. These two factors are more significant than the age and education of consumers. Therefore, it can be reasoned that the act of selling, auctioning or buying goods online is a risky routine activity that will increase the likelihood of being victimized in cyberspace, which is consistent with the theories discussed above.

Moreover, research shows that increased usage of SNS tends to increase the probability of convergence between motivated offenders and suitable victims in cyberspace (Reyns et al., 2011). Interestingly, however, Saridakis et al. (2016) find that individuals who have a higher usage of dominant multipurpose social media sites (e.g. Facebook and Google+) are less likely to be victims of cybercrimes. However, the study also finds that individuals who have higher usage of knowledge-sharing through social media (e.g. LinkedIn, Twitter and Blogger) are more likely to become victims of cybercrime. These findings could be explained through the psychology of human behavior since the public mindfulness of the inherent risk associated with dominant social media sites may cause them to take additional precautions compared to the perceived level of trust and safety associated with knowledge-sharing social media sites where they may take less precautionary or safety measures. Furthermore, Saridakis et al. (2016) show that higher computer skills and greater technological efficacy is positively but statistically insignificantly related to victimization. The researchers argue that the positive relationship could be due to the individual perception of their superior computer skills resulting in an increased risk-taking behavior that exposes them

to higher probabilities of victimization. This finding is consistent with Gottfredson and Hirschi's GTC since this can be viewed as a preference for risk-taking behavior, which is an element of low self-control, therefore this characteristic increases the individual likelihood of being victimized.

CONCLUSION

There are several theories outlined in this chapter, which include, the RAT, the GTC, the DPT and the RCT, all of which attempt to address the phenomenon of human behavior that leads us to commit an act of crime. The desired approach to crime should not be merely to catch the offenders of crime but to prevent the occurrence of a crime by addressing and removing the stimuli that encourage or allow it to happen. All these theories of crime have been modified and extended to include the new age of cyber-crime especially in the financial sector and among all individuals using SNS.

To gain better insights in addressing evolving challenges of the digital world, cybersecurity increasingly relies on advances in research done on human behavior. Whilst technology may often form the core of cyber-attacks, these incidents are instigated by and responded to by people. Researchers believe that SNS are important tools that promote social exchange since social interaction plays a vital role in education (Vollum, 2014, as cited in Benson, 2015c). Therefore, strategies should be developed to minimize the risk of cyberattacks which will allow the continued use of SNS to promote social interactions in a safer cyberspace. Researchers also need to address the issue of privacy since privacy on SNS is not only an individual issue but also an organizational and institutional one that involves data sharing actors (Benson et al., 2015a). The number of registered social network users and the amount of time spent on social network increase every year. In addition, the commercial value of personal information on SNS is on the rise (Benson et al., 2015a) having a tangible contribution to the digital economy. Therefore, with this growing rate of technology and increased dependence on the internet for SNS and other essential functions, our risk of losses due to cybercrime is continuously increasing.

Strategies to be used in the protection against cyberattacks can be intelligently developed and delivered by the government awareness programs, public places and on television to raise awareness of cybercrime. For example, a study by Marcum et al. (2010) suggests that youths lower their probability of online victimization by communicating only with people whom they know on SNS, and not giving personal information to people that they do not know. Furthermore, by gaining a better understanding of the human aspect of cybercrime through psychology, we can develop better mitigation strategies for cybercrimes. This area of human element exploration has a big impact on the future of computing. As such, the younger generation is driving the commercialization of social media platforms. Therefore, gaining a better understanding of their behavioral traits, intentions and acquisition of safe usage patterns are imperative for the prevention of criminal exploitation of the young user of SNS.

RESEARCH QUESTIONS OPEN FOR FURTHER DISCUSSION

This chapter ends with a series of questions warranting future research to explore. These include:

- Should strategies be adopted based on the target age group, as different age groups have different online skills and use the internet for different purposes?
- Do geographical location, technological literacy and culture play a role in determining the types of cybercrime activities?
- Does the risk of losses due to cybercrime activities outweigh the efficiency benefit of implementing the emergent digital technology offerings?
- Can a connection between suicide incidents, mental-illness, cyber-bullying or identity theft cases be established by researchers?
- Governments have placed significant emphasis on privacy regulation. Should they continue to regulate the privacy controls of SNS or leave it up to the owners of the SNS to prioritize data commercialization over individual privacy?

This is the time when academic attention is so valued, having the potential to mitigate future cyberattacks, as well as minimize their impact on individuals who are yet to realize their full potential in business and enter the workforce. In order to take control of online victimization, the relevant stakeholders, including policy makers and SNS vendors, need to have sufficient control and public awareness to support a safer online future for the younger generation.

REFERENCES

- Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2019). The Welfare Effects of Social Media. *National Bureau of Economic Research*. Working Paper 25514. Retrieved from <https://www.nber.org/papers/w25514.pdf>
- Benson, V. (2017). *The State of Global Cyber Security: Highlights and Key Findings*. London, UK: LT Inc. doi:10.13140/RG.2.2.22825.49761
- Benson, V., Saridakis, G., & Tennakoon, H. (2015a). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People*, 28(3), 426–441. doi:10.1108/ITP-10-2014-0232
- Benson, V., Saridakis, G., & Tennakoon, H. (2015c). Purpose of social networking use and victimisation: are there any differences between university students and those not in HE? *Computers in Human Behavior*, 51(B), 867–872.
- Benson, V., Saridakis, G., Tennakoon, H., & Ezingear, J. N. (2015b). The role of security notices and online consumer behaviour: An empirical study of social networking users. *International Journal of Human-Computer Studies*, 80, 36–44. doi:10.1016/j.ijhcs.2015.03.004
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. doi:10.2307/2094589

Culnan, M. J., McHugh, P. J., & Zubillaga, J. I. (2010). How Large U.S. Companies Can Use Twitter and Other Social Media to Gain Business Value. *MIS Quarterly Executive*, 9(4), 243–259.

Eck, J. E., & Clarke, R. V. (2003). Classifying Common Police Problems: A Routine Activity Approach. *Crime Prevention Studies*, 16, 7–39.

Facebook. (2018). *Facebook Newsroom - Company Info*. Retrieved from <https://newsroom.fb.com/company-info/>

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Hansen, J., Saridakis, G., & Benson, V. (2017). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior*, 80, 197–206. doi:10.1016/j.chb.2017.11.010

Hill, M. S., & Duncan, G. J. (1987). Parental family income and the socioeconomic attainment of children. *Social Science Research*, 16(1), 39–73. doi:10.1016/0049-089X(87)90018-4

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20–40. doi:10.1080/01639625.2013.822209

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, 26(2), 107–122. doi:10.1080/08946566.2013.821809 PMID:24499279

Kaplan, A. M., & Haenlein, M. (2010). Users of the World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons*, 53(1), 59–68. doi:10.1016/j.bushor.2009.09.003

Kuss, D. J., & Griffiths, M. D. (2011). Online Social Networking and Addiction—A Review of the Psychological Literature. *International Journal of Environmental Research and Public Health*, 8(9), 3528–3552. doi:10.3390/ijerph8093528 PMID:22016701

Kuss, D. J., & Griffiths, M. D. (2017). Social Networking Sites and Addiction: Ten Lessons Learned. *International Journal of Environmental Research and Public Health*, 14(3), 311. doi:10.3390/ijerph14030311 PMID:28304359

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior*, 31(5), 381–410. doi:10.1080/01639620903004903

McAfee. (2018). Executive Summary: The Economic Impact of Cybercrime-No Slowing Down. *McAfee Research 2018*. Available at: <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf>

McAlaney, J., Frumkin, L., & Benson, V. (2018). *Psychological and Behavioral Examinations in Cyber Security*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-4053-3

McLanahan, S. (1985). Family structure and the reproduction of poverty. *American Journal of Sociology*, 90(4), 873–901. doi:10.1086/228148

Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *Cyberpsychology & Behavior*, 12(4), 387–393. doi:10.1089/cpb.2009.0068 PMID:19630583

Pew Research. (2015). The Demographics of Social Media Users. *Internet & Technology*. Retrieved from <http://www.pewinternet.org/2015/08/19/the-demographics-of-social-media-users/>

Pew Research. (2018). Social Media Use in 2018. *Internet & Technology*. Retrieved from <https://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>

Piquero, A. R., Macdonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime. *Journal of Quantitative Criminology*, 21(1), 55–71. doi:10.1007/10940-004-1787-2

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), 267–296. doi:10.1177/0022427810365903

Reyns, B., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, 38(11), 1149–1169. doi:10.1177/0093854811421448

Saridakis, G., Benson, V., Ezingard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320–330. doi:10.1016/j.techfore.2015.08.012

Schaefer, L., & Mazerolle, L. (2017). Putting Process into Routine Activity Theory: Variations in the Control of Crime Opportunities. *Security Journal*, 30(1), 266–289. doi:10.1057j.2015.39

Schreck, C. J. (1999). Criminal victimisation and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*, 16(3), 633–654. doi:10.1080/07418829900094291

Siegel, L. J. (2006). *Criminology* (10th ed.). University of Massachusetts, Lowell.

Statista. (2018). Global digital population as of October 2018 (in millions). *Demographics & Use*. Available at: <https://www.statista.com/statistics/617136/digital-population-worldwide/>

Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2010). *Digital crime and digital terrorism* (2nd ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Tennakoon, H., Saridakis, G., & Mohammed, A.-M. (2018). Child Online Safety and Parental Intervention: A Study of Sri Lankan Internet Users. *Information Technology & People*, 31(3), 770–790. doi:10.1108/ITP-09-2016-0213

Williams, M. L. (2015). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology*, 56(1), 21–48. doi:10.1093/bjc/azv011

KEY TERMS AND DEFINITIONS

5

Cyber Security: Cyber security is the protection of internet-connected systems, including hardware, software, and data from cyberattacks.

Cyber Security Skills: Cyber security skills are those skills associated with ensuring the security of information technology (IT-generally referring to information storage and integrity) and operational technology (OT-referring to systems that control physical devices).

Cyber-Victimization: Cyber-victimization refers to the process in which others are victimized through the use of information and communication technologies.

Cyberattack: A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.

Cybercrime: A cybercrime is any criminal activity that involves a computer a networked device or a network.

Risky Online Behavior: A risky online behavior is an action that can potentially leave one exposed to a variety of dangers, putting individual and possibly organizational internet security at risk.

Social Network: A social network is an online communication platform that is used for creating relationships with other people who share an interest, background or real relationship.

Online Expression, Personal Cybersecurity Costs, and the Specter of Cybercrime

Juhani Rauhala

University of Jyväskylä, Finland

Pasi Tyrväinen

 <https://orcid.org/0000-0001-7716-3244>

University of Jyväskylä, Finland

Nezer Zaidenberg

College of Management Academic Studies, Israel

INTRODUCTION

The UN General Assembly has declared freedom of expression to be a universal human right (UN General Assembly, 1948). As of 2016, the United Nations has resolved that unrestricted access to the Internet is also a human right (UN Human Rights Council, 2016). A commonly accepted benefit of the Internet is that it serves as a platform for free expression. Importantly, political topics are also discussed as well as other topics without socially accepted *savoir faire*. However, there are potential consequences for users who make controversial or provocative expressions over the Internet from other users and organizations participating in or following the communication (Baroni, 2015; Cassidy, 2017; Jaschik, 2014). Such consequences may also be in the form of illegal doxing or hacking attacks by cybercriminals.

Users' concerns about such consequences may have an inhibiting effect on their Internet usage for free expression. This inhibiting effect may correlate with what users believe and how users behave concerning addressing security and privacy issues of their devices. The inhibiting effect may also correlate with users' attitude toward and perception of the time they spend addressing their devices' security and privacy issues. However, the association between online expression aspects and the perception of time consumption on security aspects is lacking in prior research. Users may be reluctant to express themselves online simply because anonymity costs too much time and effort. That is, the users may be aware of the importance and abundance of tools providing anonymity and may wish to express themselves online but decide that spending time on anonymity is just too much effort. Concern about such consequences may not only have an inhibiting effect on users' use of the Internet for expression but it may also correlate with their desire to purchase personal cybersecurity products and anonymizing services.

Another generally accepted beneficial use of the Internet is as a platform for commerce, which is continuously increasing (Emarketer.com, 2014). At the same time, spending by consumers and businesses on cybersecurity products and services is also increasing (Morgan, 2017). It is reasonable to expect that users purchase a significant proportion of personal cybersecurity software online. It is possible that misgivings of users about the Internet as a platform for free expression may correlate with increased Internet utilization by those same users for commerce in personal cybersecurity products and services. This article explores this somewhat paradoxical relationship given that the Internet is seen as an overall good for humanity. It leads to a focus of this chapter; that is, to the consideration of users' reluctance

DOI: 10.4018/978-1-5225-9715-5.ch067

to express themselves in relation to their attitudes and perceptions regarding the time and money they invest in security. This is relevant to participation in social media and other online expression contexts.

To facilitate research and discussion on this topic, six latent factors are elucidated: three corresponding to a reluctance to self-express online, one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount ("too much") of one's time, and one for time considering device cybersecurity and privacy settings aspects. The sixth factor corresponds to a positive predilection toward personal spending to enhance personal cybersecurity. The correlation among two of these factors is then analyzed. A linear regression of one latent factor against the other and against a demographic factor is also performed.

This chapter presents an overview of related research, followed by a description of a proposed research model. It then establishes the general latent factors. Some results are presented and discussed, followed by a description of future research suggestions, and a conclusion.

BACKGROUND

Previous research has considered implications on free expression and the benefits of free expression. Willingness to express opinions online has been measured in terms of a web forum's view/reply ratio (Shen & Liang, 2015) and by asking users how likely they would be to express their opinions in specified online scenarios using a 0-100% or 0-10 scale (Ho & McLeod, 2008; Stoycheff, 2016). Hayes et al. (2005) established a self-reporting tool consisting of eight five-point Likert questions to measure willingness to self-censor. However, the tool's questions pertain to a general social context and not specifically to self-expression of controversial opinions on the Internet. Attempts to measure a reluctance to express on the Internet or to establish the same as a latent factor are lacking in previous research.

The emerging research of Booth (2017) has raised attention to the issue of freedom of expression and the laws and norms thereof in terms of their relationship to the benefits of ICT on national well-being. However, her research does not consider the relationship between the expression of free speech on aspects of the individual user. Internet communication is largely beyond the territorial control of the nation-state and access to the Internet has been recognized as important to the freedom of expression and to participation in a democracy (Lucchi, 2011). Previous research has established that usage of the Internet for free expression can be a way of circumventing censorship or other hindrances that prevent citizens' freedom of expression in more traditional publishing media, especially in authoritarian regimes (Nadi & Firth, 2004).

Prior research has shown that many states have begun imposing online surveillance upon their citizens by way of legislative acts or other means (Ray & Kaushik, 2017). The research suggests that the ostensible justifications for such surveillance, such as cyberterrorism or cybercrime, are questionable and disproportional to the scope of the surveillance desired by the state. Such surveillance does not directly restrict online expression but it can create hesitation or concern in the user. The user may hesitate to criticize the state or its policies in an online forum due to fear of being surveilled. Many states also impose varying levels of censorship and controls on online expression (Ray & Kaushik, 2017).

Debate and discussions that occur over online forums and social media, such as Twitter and Facebook, are raising the attention to a virtually unlimited array of topics. Importantly, socially controversial topics and political topics are also discussed. Certain organizations consider and evaluate the various threats to the freedom of expression online (Stanton, 2014). In oppressive states, free expression enabled by access to the Internet can be particularly important for advancing human rights (Nadi & Firth, 2004).

However, there are potential consequences for users who make controversial or provocative expressions on the Internet, including a negative reaction from the government (Baroni, 2015; Cooper, 2000; Mony, 2017) and offended individuals (Cassidy, 2017), employers (Jaschik, 2014), and schools (Curtom, 2014). Consequences may also be exacted by vindictive criminal hackers. Cybercrime against individuals has been defined as: “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)” (Halder & Jaishankar, 2012). Victims may become a topic for cybercriminal gangs in the Deep Web or the target of doxing. “Revenge hacking” and doxing have caused serious consequences to victims (Branigan, 2011; Dascalescu, 2018). Participating in social media is a form of individual expression and there is some research-in-progress on the effects of perceived security threats on user’s social media behavior (Alqubaiti et al., 2016).

Users spend significant time performing self-protective cybersecurity and privacy-related tasks. This time detracts from the amount of time users have available for other preferred activities. For example, when using open WiFi connectivity in a public space or vehicle, spending time connecting to a secure VPN or updating the security software will leave less time for messaging and for checking social media updates. The excess use of time spent waiting can be merely a perception but may still have negative consequences in terms of user experience or perception of the services for which the waiting is done (Dellaert & Kahn, 1999). Another study has been performed to determine how consumers react when web pages of shopping websites take too much time to load (Anonymous, 2010). It found that 70% of respondents reported that they abandon shopping on a site if the site takes more than 10 seconds to load and 35% said they would not return if the loading delays take “too long.” On the other hand, the tolerance of users to the amount of time spent waiting will vary according to the individual and the context (Katz & Martin, 1989). During Internet usage, a loading delay may be experienced with most mouse-clicks or screen taps. However, the need to spend time waiting for a security software update process to complete occurs relatively infrequently, e.g. weekly or monthly.

Excessive non-ideal time consumption, therefore, can be said to detract from more desirable activities and may cause a negative perception of offerings associated with waiting. Frustration with excessive time consumption can result in a negative attitude toward, and possibly abandonment of, desirable online content and activities.

Controversial expression in an online communications context is affected by other factors. Such factors include perceived anonymity and familiarity with other online community participants (Luarn & Hsieh, 2014). Luarn and Hsieh studied the expression behavior of users in a laboratory-controlled virtual community. The virtual community simulated different online group communications environments. They found that users were more willing to express controversial opinions when their identities were anonymous or when they were familiar with other members of the community. When users in the study were not anonymous, they were more reluctant to express such opinions. They also found that there was no effect of anonymity or member familiarity on users’ willingness to express non-controversial opinions.

Prior research has shown that negative expressions are received differently than neutral or positive ones. Kwon et al. (2013) studied communications and expressions in a messaging context. They examined the acceptability of negative communications. They found that emotional expressions that accompany negative communications were considered much less acceptable than emotional expressions in positive ones. Negative messages by their nature are less welcome. Negative expressions (e.g., unpleasant or aggressive) can result in unwanted consequences. Internet users may be reluctant to express themselves

because of concerns about such consequences. The time they spend on personal cybersecurity issues may further discourage their controversial expressionism.

It is of note that Booth and other researchers utilize the Human Freedom Index (HFI) (Vasquez & Porcnik, 2017). Included in the HFI measures are those that measure freedom of expression. Among those measures are “Laws and Regulations that Influence Media Content,” “Political Pressures and Controls on Media Content,” and “State Control over Internet Access.” The measures of Laws and Regulations that Influence Media Content and Political Pressures and Controls on Media Content could be useful for this study on the condition that they are applied indirectly. That is to say, for example, that an assumption would be that an average user would feel some reluctance to freely express themselves as a result of the laws and controls. This study addresses reluctance more directly in the survey questions, whereas the subset of HFI measures does not measure reluctance to express. The HFI’s “expression freedom” measures have not been examined for their relationship to personal cybersecurity spending. In particular, they do not measure concern regarding the consequences of personal free expression and neither have they been analyzed for their relationship to Internet users’ attitudes and behaviors toward purchasing personal cybersecurity protections.

There are also studies observing the impact of demographic factors, such as nationality and age, on Internet behaviour that are relevant to this study. Regan, FitzGerald, and Balint (2013) have evaluated attitudes toward information privacy between age groups (specifically generations). Their analysis revealed a trend where younger generations tend to be more concerned than older ones about wiretapping and data privacy. Chen, Hsu, and Lin (2010) determined that consumers with different levels of computer expertise have different preferences for attributes of shopping websites. Research into culture-based differences in perception of risk for online shopping and other tasks has yielded conflicting results (Sims & Xu, 2012). Sims and Xu (2012) found no significant difference between the UK and Chinese shoppers’ perceived risk of online shopping despite those shoppers’ differing cultural backgrounds. This conclusion was against their expectations and the contradicted results from prior research that showed differences in risk-aversion between the two cultures (Hofstede, 1980).

Sheehan (2002) found that users’ education and age correlate with their level of concern about online privacy. Hazari and Brown (2013) studied whether demographic variables can affect Internet users’ privacy concerns and, thus, their attitudes toward using social networking sites. In contrast to the results from Sheehan and from Regan, Fitzgerald, and Balint, their research found that age was not correlated with online privacy concerns. Bandyopadhyay (2011) found that factors such as the level of Internet literacy, social awareness, and cultural background affect Internet users’ online privacy concerns. He found that among the possible consequences of such concerns is an unwillingness to use the Internet. Liu et al. (2016) applied social exchange theory to examine perceived risks and rewards of individual users’ self-disclosure in social media. The authors found that perceived privacy risk can reduce the willingness of social media users to disclose personal information. There does not seem to be existing research on social exchange theory applied to controversial expression by individual users online. Previous work has examined the effect on willingness to disclose information about oneself. Based on previous research, it can be hypothesized that the reluctance to express oneself on the Internet may be connected with concerns about the consequences. Further, reluctance to express oneself may lead to the use of cybersecurity as a means to protect oneself in these cases. However, there seems not to be previous results addressing this hypothesis.

Previous research has attempted to address the monetary and non-monetary costs of consumer-facing cybercrime (Riek & Böhme, 2018). The research focused on cybercrime incidents such as scams and payment fraud. The costs in Riek and Bohme's research are not the costs of the fear of consequences that could result from expressing oneself online. The feared consequences in the RtoEx subfactor of this study are unspecified and general. They may occur in varying forms including, but not limited to, cybercriminal attacks against the user.

The authors believe that it is important to consider the attitudes of users toward free expression on the Internet and possible consequences resulting from users' reluctance to freely express themselves on the Internet.

RESEARCH MODEL

This study proposes six latent factors: three corresponding to a reluctance to self-express online (RtoEx), one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount of one's time (TMT, from "too much time"), and one corresponding to the performance of checking and changing device privacy and security settings (TChS, from "think about and change settings").

The factors are:

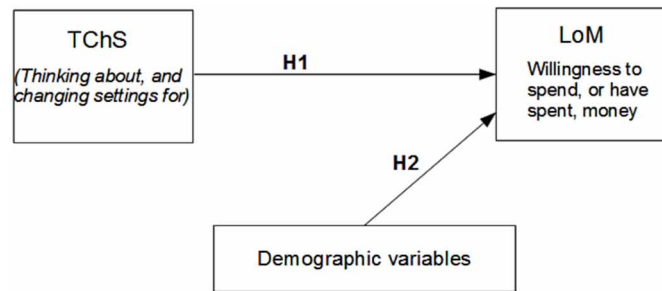
- **Reluctance to Express (RtoEx):** Reluctance to freely self-express online. The reluctance of expressing can be further divided into two factors based on inclusion or exclusion of consequences of the expression, RtoExC and RtoExnonC, respectively.
- **Reluctance to Express When Consequences Mentioned (RtoExC):** Reluctance to Express due to concerns of possible Consequences or safety; The reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.
- **Reluctance to Express When Consequences Not Mentioned (RtoExnonC):** Reluctance to Express when users are not reminded of possible Consequences or safety issues resulting from the expression.
- **Too Much Time (TMT):** The belief that cybersecurity risk amelioration requires excessive usage of one's time
- **Think Change Settings (TChS):** Time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether the time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.
- **Loss of Money (LoM):** Personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

As a demonstration, the authors hypothesize that those users who are conscientious about their online security and privacy will spend both time and money to ensure it. This should be reflected in a significant correlation between TChS and a positive attitude toward purchasing personal cybersecurity products and services (or LoM, for "Loss of Money")(Figure 1).

H1: TChS will be correlated with a positive attitude toward purchasing personal cybersecurity products and services (LoM).

H2: TChS combined with one or more demographic variables will predict LoM.

Figure 1. Latent variables TChS and LoM, and independent demographic variable(s)



Latent Factors and Their Indicators

Each of the latent variables can be derived from sets of indicator questions. Indicator questions for TChS and LoM were included in a survey, and each consisted of responses along a five-point Likert scale from “strongly agree” to “strongly disagree.” For data gathering, a survey was administered over the Web to a population composed mainly of Finnish university students and working adults. 191 responses were obtained.

The questions for TMT were as follows: five questions to assess the perception that excessive time has been spent addressing device security and privacy issues and a belief that time spent on device security and privacy aspects has detracted from time intended for other tasks. TChS is established with three questions to assess whether the user has contemplated and checked (and perhaps adjusted) their device’s security and privacy settings (available from the authors). Cumulatively, the authors suggest the five “too much time” indicator questions imply that the respondent spends time contemplating and actively addressing security and privacy aspects but tends to feel negative about doing so.

The survey included questions on respondents’ behaviors and attitudes regarding personal spending on cybersecurity. Latent variable Loss of Money (LoM) is defined by responses to a set of four indicator questions. The questions for LoM are designed as follows: two questions to ascertain whether the respondent/subject has purchased to enhance his cybersecurity and two questions to ascertain the general attitude of the respondent toward security software purchases (available from the authors). Cumulatively, it is suggested the LoM indicator questions indicate the willingness to buy software products or services that enhance personal cybersecurity.

An Exploratory Factor Analysis with direct oblimin rotation is used to extract latent components from a set of survey questions. The results for TMT, TChS, and LoM confirm three components. Review of the corresponding survey questions indicates that the TMT and TChS responses are differentiated by the mention of security issues detracting time from preferred tasks, or by a belief that addressing security issues takes too much of one’s time (Table 1).

A Spearman correlation analysis is performed on the indicator question responses corresponding to TMT (five questions), TChS (three questions), and LoM (four questions). All of the responses within the three respective sets of indicator questions have two-star Spearman correlations with each other (Table 1). Because the indicator questions for the three latent variables have high intercorrelation, the mean scores of the responses were computed and utilized for analysis. SPSS statistical software was used to calculate Pearson correlations between the latent variables as well as the Cronbach’s alphas. The Cronbach’s alpha values show acceptable reliability between the latent variables’ indicators (Table 1).

Table 1. Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor; mean correlations; and Cronbach's alpha

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
TChS	.319**	.485**	.407	.673
TMT	.221**	.772**	.405	.766
LoM	.500**	.863**	.639	.871

Results for TChS and LoM

Analysis of the results (Table 2) for the TChS vs. LoM hypothesis shows a significant correlation, thus H1 is confirmed.

Regression analysis is performed on LoM as the dependent variable against some demographic variables. The analysis shows some correlation with the combination of TChS and age (adjusted R squared = .035, p-value = .013). H2 is therefore valid for age.

When the model is properly applied, hypotheses utilizing the other latent factors may be similarly evaluated.

SOLUTIONS AND RECOMMENDATIONS

From the viewpoint of encouraging open and robust political discourse, governments should ensure the framework and conditions for free expression by their citizens with online regulatory safeguards that correspond to the traditional safeguards in traditional communications media. This could help Internet users feel freer to spend money and time on personal interests instead of diverting spending due to concerns about their online privacy and security. If users would have less reason to be worried about becoming victims of cybercrime, they could spend more time expressing themselves and exploring offerings. In these ways, online merchants could benefit from more confident online consumers, and societies could benefit from the desired online discourse.

The HFI may be enhanced by the inclusion of a measure to assess citizens' reluctance to express legal, but controversial, viewpoints online. Citizens may be reluctant to express such viewpoints despite states' official policies allowing free expression. The concern about consequences resulting from such expression may not necessarily align with states' official policies and the possibility of state-imposed consequences does not necessarily align with states' official policies. The current HFI does not account for citizens' concerns and perceptions of these issues.

In the analysis, some differences between nationalities in the responses were noted. However, further data should be collected. One direction to search for a potential explanation is cultural differences (Hofstede, 1980).

Table 2. Pearson correlation between LoM and TChS. Two-tailed significance: * to 0.05 level

	n	Spend time thinking about and changing settings (TChS)
LoM	191	.160*

Better default security and privacy settings could reduce the perceived need for purchasing supplemental personal cybersecurity solutions. This would free up more time and money for users to apply to preferable tasks and transactions. Ideally, users should be confident that their devices have sufficient privacy and security protection “out of the box”. Prior research has shown that users’ trust in the safeguarding of their privacy and security is positively related to their online purchase intentions (Chen & Barnes, 2007).

FUTURE RESEARCH DIRECTIONS

Applied social exchange theory could be expanded to account for Internet users’ reluctance to freely express their thoughts and opinions online. Further research could explore the factors that inhibit users from expressing controversial viewpoints and factors that encourage such expression online.

The indicator questions used in the demonstration study did not examine how, in the case of waiting, the management of time affects the perspective of the person waiting. Examples of such cases could be the users’ management of the time spent waiting for a security software update to install; or the content displayed on screen by the software during the update (Hanyang, et al., 2015).

For the TChS vs LoM hypothesis, future research could examine the impact of attitudes toward, and usage of, free and open source personal cybersecurity solutions. Users who believe they can achieve acceptable levels of personal cybersecurity with free tools would not necessarily be purchasing such tools. This could affect the LoM factor and thus the significance of the correlation between LoM and TChS. Regression analysis showed that age affects the TChS vs LoM correlation. Younger users who take time to contemplate their device settings feel more positive about spending money on personal cybersecurity.

This demonstration study did not consider free and open source personal cybersecurity products and tools that are available. Such tools include Tor browser, ClamAV, and free VPN services. Some respondents may have responded negatively to the survey questions regarding spending because they believe that they can achieve sufficient personal cybersecurity without spending money doing so. Future studies could account for such products.

Using the proposed research model and introduced latent variables, research can be performed to determine the effects of some independent variables (e.g., income and ICT expertise) on the relationships between the latent variables. Research can explore the relationship of certain demographic variables to personal cybersecurity spending and to any reluctance to express oneself online. Users could also be surveyed to directly gauge their concern about being victimized by cybercriminals as a result of their expressions. Subject to available survey data, analysis for geographical region clustering and other clusterings could also be performed.

CONCLUSION

While sales of cybersecurity products and services are suitable for the cybersecurity industry, they also indicate the real cybersecurity concerns of Internet users. Many Internet users go online, but may then be reluctant to freely express themselves, spending their time and money to alleviate perceived cybersecurity risks from political vigilantes, cybercriminals, or other entities. This scenario is not the ideal or optimal use of the Internet by society. Future research can investigate methods to encourage free expression online and reduce the perceived risks of such free expression.

In this chapter, an overview of research pertaining to the chapter topic was presented, and a simple research model was proposed. Six latent factors were proposed; three corresponding to a reluctance to self-express online (RtoEx, RtoExC, and RtoExnonC); one corresponding to a belief that handling the security and privacy aspects of one's device requires an excessive amount of one's time, TMT; one for time considering device cybersecurity and privacy settings aspects, TChS; and one for personal cybersecurity spending, LoM. Based on the factor analysis of the responses to some indicator statements, TChS and LoM were established.

A study using two of the latent variable showed a significant correlation between TChS and LoM, thus hypothesis H1 is confirmed. The association transcended nationality. The correlation was significant only when the entire response set was analyzed. Analysis by nationality did not show a significant correlation for any of the three most prominent nationalities of survey respondents. Regression analysis showed that age and TChS are predictors of LoM. Hypothesis H2 is therefore confirmed for age. Younger users who are conscientious about their device privacy and security settings are more likely to spend money on personal security or feel more positively about doing so.

REFERENCES

- Alqubaiti, Z., Li, L., & He, J. (2016). The Paradox of Social Media Security: Users' Perceptions versus Behaviors. In *Proceedings of the 5th Annual Conference on Research in Information Technology - RIIT '16* (pp. 29–34). Boston: ACM Press. doi:10.1145/2978178.2978187
- Anonymous. (2010, January). Keeping online customers. *Dealerscope*, 52(1), 26. Retrieved from <https://search-proquest-com.ezproxy.jyu.fi/docview/218956873?accountid=11774>
- Bandyopadhyay, S. (2011). Antecedents And Consequences Of Consumers Online Privacy Concerns. *Journal of Business & Economics Research*, 7(3). doi:10.19030/jber.v7i3.2269
- Baroni, D. (2015, July 3). New Zealand Government To Punish Online Trolls With Prison Time. Retrieved from <http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time>
- Booth, R. E. (2017). The Effect of Freedom of Expression and Access to Information on the Relationship between ICTs and the Well-being of Nations. *Proceedings of the 23rd Americas Conference on Information Systems*.
- Branigan, S. (2011, July 31). Revenge Hacking. Retrieved May 17, 2019, from Trends in high tech security website: <https://sbranigan.wordpress.com/2011/07/31/revenge-hacking/>
- Cassidy, P. (2017, November 3). Man petrol bombed homes in revenge for Facebook post. STV News. Retrieved from <https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/>
- Chen, Y., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management & Data Systems*, 107(1), 21–36. doi:10.1108/02635570710719034
- Chen, Y.-H., Hsu, I.-C., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of Business Research*, 63(9–10), 1007–1014. doi:10.1016/j.jbusres.2009.01.023

Cooper, A. K. (2000, July 12). China: Government punishes Internet journalists. Committee to Protect Journalists. Retrieved from <https://cpj.org/2000/07/china-government-punishes-internet-journalists.php>

Curtom, G. (2014, April 24). Students punished for expressing free speech on Twitter. The Cougar. Retrieved from <http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/>

Dascalescu, A. (2018, January 3). Doxxing Can Ruin Your life. Here's How (You Can Avoid It). Retrieved May 17, 2019, from Heimdal Security website: <https://heimdalsecurity.com/blog/doxxing/#doxxingswatting>

Dellaert, B. G. C., & Kahn, B. E. (1999). How tolerable is delay?: Consumers' evaluations of internet web sites after waiting. *Journal of Interactive Marketing*, 13(1), 41–54. doi:10.1002/(SICI)1520-6653(199924)13:1<41:AID-DIR4>3.0.CO;2-S

Emarketer.com. (2014). Worldwide Ecommerce Sales to Increase Nearly 20% in 2014 - eMarketer. Retrieved November 22, 2017, from <https://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039>

Halder, D., & Jaishankar, K. (2012). *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations*; doi:10.4018/978-1-60960-830-9

Hayes, A. F., Glynn, C. J., & Shanahan, J. (2005). Validating the Willingness to Self-Censor Scale: Individual Differences in the Effect of the Climate of Opinion on Opinion Expression. *International Journal of Public Opinion Research*, 17(4), 443–455. doi:10.1093/ijpor/edh072

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, 9(4), 31–51. doi:10.1080/15536548.2013.10845689

Ho, S. S., & McLeod, D. M. (2008). Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication. *Communication Research*, 35(2), 190–207. doi:10.1177/0093650207313159

Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values* (1st ed.). Beverly Hills, CA: Sage Publications.

Jaschik, S. (2014, September 15). Interview with professor fired by West Bank university who compares himself to Steven Salaita. Inside Higher Ed. Retrieved from <https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita>

Katz, K. L., & Martin, B. R. (1989). Improving customer satisfaction through the management of perceptions of waiting. Massachusetts Institute of Technology. Retrieved from <http://hdl.handle.net/1721.1/37703>

Kwon, O., Kim, C., & Kim, G. (2013). Factors affecting the intensity of emotional expressions in mobile communications. *Online Information Review*, 37(1), 114–131. doi:10.1108/14684521311311667

Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management*, 53(1), 53–63. doi:10.1016/j.im.2015.08.006

Luarn, P., & Hsieh, A.-Y. (2014). Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities. *Online Information Review*, 38(7), 881–895. doi:10.1108/OIR-03-2014-0076

Lucchi, N. (2011). Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. *ARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, 19(3), 645–678.

Luo, H., Wang, J., Han, X., & Zeng, D. (2015). The impact of filler interface on online users' perceived waiting time. In 2015 12th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1–5). Guangzhou, China: IEEE. 10.1109/ICSSSM.2015.7170198

Mony, S. (2017, November 11). Cambodian Netizens Face New Risks as Government Tightens Online Controls. VOA. Retrieved from <https://www.voanews.com/a/cambodian-netizens-new-risks-governmentonline-controls/4111483.html>

Morgan, S. (2017). The Cybersecurity Market Report covers the business of cybersecurity, including market sizing and industry forecasts, spending, notable M&A and IPO activity, and more. Retrieved November 22, 2017, from <https://cybersecurityventures.com/cybersecurity-market-report/>

Nadi, Y., & Firth, L. (2004). The Internet Implication in Expanding Individual Freedom in Authoritarian States. ACIS 2004 Proceedings.

Ray, A., & Kaushik, A. (2017). *State transgression on electronic expression: is it for real?* Information and Computer Security; doi:10.1108/ICS-03-2016-0024

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation (Abingdon)*, 26(1–2), 81–99. doi:10.1080/13511610.2013.747650

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates†. *Journal of Cybersecurity*, 4(1). doi:10.1093/cybsec/tyy004

Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, 18(1), 21–32. doi:10.1080/01972240252818207

Shen, F., & Liang, H. (2015). Cultural Difference, Social Values, or Political Systems? Predicting Willingness to Engage in Online Political Discussion in 75 Societies. *International Journal of Public Opinion Research*, 27(1), 111–124. doi:10.1093/ijpor/edu012

Sims, J., & Xu, L. (2012). Perceived Risk of Online Shopping: Differences Between the UK and China. In UK Academy for Information Systems Conference Proceedings (Vol. 25). Academic Press.

Stanton, L. (2014, August 18). Effect of “right to be forgotten” on free expression sparks debate. Cybersecurity Policy Report.

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*, 93(2), 296–311. doi:10.1177/1077699016630255

UN General Assembly. (1948). Universal Declaration of Human Rights. Retrieved from <https://www.un.org/en/universal-declaration-human-rights/index.html>

UN Human Rights Council. (2016). Resolution on the promotion, protection and enjoyment of human rights on the Internet. Retrieved from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Vasquez, I., & Porcnik, T. (2017). *The Human Freedom Index 2017: A Global Measurement of Personal, Civil, and Economic Freedom*. Washington, DC: Cato Institute, Fraser Institute, and the Friedrich Naumann Foundation for Freedom.

ADDITIONAL READING

Camulli, E. (2012, November 28). Customer Experience Frustration Points and Their Consequences. CMSWire. Retrieved from <https://www.cmswire.com/cms/customer-experience/customer-experience-frustration-points-and-their-consequences-018455.php>

Chua, C., Rose, G., Khoo, H. M., & Straub, D. (2005). Technological Impediments to B2C Electronic Commerce: An Update. *Communications of the Association for Information Systems*, 16.

Cushman, T. (2016). The Fate of Freedom of Expression in Liberal Democracies. *Society*, 53(4), 348–351. doi:10.1007/12115-016-0047-z

Hayes, A. F. (2005). Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research. *International Journal of Public Opinion Research*, 17(3), 298–323. doi:10.1093/ijpor/edh073

Hong, S.-B., Zalesky, A., Cocchi, L., Fornito, A., Choi, E.-J., Kim, H.-H., ... Yi, S.-H. (2013). Decreased Functional Brain Connectivity in Adolescents with Internet Addiction. *PLoS One*, 8(2), e57831. doi:10.1371/journal.pone.0057831

Kraut, R. E., Patterson, M., Lundmark, V., Kiesler, S., Mukhopadhyay, T., & Scherlis, W. (1998). Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being? *The American Psychologist*, 53(9), 1017–1031. doi:10.1037/0003-066X.53.9.1017

Rose, G. M., Evaristo, R., & Straub, D. (2003). Culture and consumer responses to web download time: A four-continent study of mono and polychronism. *IEEE Transactions on Engineering Management*, 50(1), 31–44. doi:10.1109/TEM.2002.808262

Ryan, G., & Valverde, M. (2005). Waiting for service on the internet: Defining the phenomenon and identifying the situations. *Internet Research*, 15(2), 220–240. doi:10.1108/10662240510590379

Strebel, J., O'Donnell, K., & Myers, J. G. (2004). Exploring the connection between frustration and consumer choice behavior in a dynamic decision environment. *Psychology and Marketing*, 21(12), 1059–1076. doi:10.1002/mar.20037

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138–150. doi:10.1016/j.cose.2016.02.009

KEY TERMS AND DEFINITIONS

HFI: Human freedom index; a numerical measure of the personal and economic freedom available in a country. It is measured annually. The HFI is determined from an evaluation of over 70 different indicators for each measured country.

LoM: Loss of money; personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

RtoEx: Reluctance to express; the reluctance to freely express oneself online or on the internet.

RtoExC: Reluctance to express due to concerns of possible consequences or safety; the reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.

RtoExnonC: Reluctance to express when users are not reminded of possible consequences or safety issues resulting from the expression.

Social Exchange Theory: A behavioral theory that seeks to explain the interaction between a person and another person or entity. Its fundamental proposition is that the interaction is influenced by the person's evaluation of the interaction's risks versus rewards.

TChS: Thinking about and changing settings; time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.

TMT: Too much time; the belief that cybersecurity risk amelioration requires excessive usage of one's time.

Leveraging on Digital Footprints to Identify Potential Security Threats: Insights From the Behavioural Sciences Perspective

Loo Seng Neo

Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

INTRODUCTION

The growing pervasiveness of the internet has revolutionised how individuals communicate and interact with one another. Despite being an effective channel for communication, it has also been exploited by individuals with malicious intent – such as criminals, violent extremists – for the purposes of fundraising, recruitment, propaganda creation and dissemination, sharing of vital information, data mining, etc. With the ease of accessibility and cloak of anonymity, individuals with malicious intent have reorganised their operations online to exist and operate in social environments that may not agree with their activities.

Violent extremists of all affiliations have exploited this technological advancement to transform the way they operate on a historically unprecedented scale. As Weimann (2004) posited, “Islamists, Marxists, nationalists and separatists, racists and anarchists all find the internet alluring” (p. 3). The internet and the opportunity it offers, allow violent extremists to expand the functionalities of their propaganda efforts beyond that the boundaries of the traditional, mainstream media (Europol, 2014). Violent extremists are no longer dependent on traditional media outlets to disseminate their propaganda. For example, it offers the opportunity for violent extremists such as Al-Qaeda in Iraq leader, Abu Musab al-Zarqawi to shape their audience worldviews. Before al-Zarqawi began his online propaganda campaign, it is essential to note that he would have to kill large numbers of people in order to grab the attention of supporters and media (Conway, 2007). However, through the online disseminations of video-taped beheadings of foreign hostages such as Nicholas Berg, al-Zarqawi was able to achieve greater impact and media publicity albeit using fewer resources. The internet has provided him with a readymade audience to exert his influence and presence. The use of the internet by individuals with malicious intent such as violent extremists therefore demands the attention of law enforcement agencies across the world.

In fact, the continuous advancement in information and communications technology can be envisioned to have a dramatic impact on the way such persons of interest may operate. Some recent examples include the online expression of hate during the 2018 Sri Lanka Kandy Riots (Gan, Neo, Chin, & Khader, 2018); acts of insider threats such as WikiLeaks data breach by Bradley Manning (Savage, 2013); online recruitment of members by violent extremist groups (Neo, Dillon, & Khader, 2017); ransomware attacks like ‘WannaCry’ (Tan & Wang, 2017); spread of fake news during the U.S. 2016 Presidential Election (Chen, Tan, Goh, Ong, & Khader, 2018); online circulation of upskirting photos (Luo & Wang, 2018); acts of cyberattacks (Dillon, 2016); and use of spear phishing to gain illegal access to computer networks (Vishwanath, 2016).

As the world witnesses an upward trend of such crime and security concerns in the online sphere, it places additional ‘responsibility’ on intelligence and law enforcement agencies to respond with the appropriate technological interventions (Abdul Rahman, 2019). Because the internet has played an im-

DOI: 10.4018/978-1-5225-9715-5.ch068

perative role in the way malicious activities are being conducted, these security agencies are therefore compelled to transform the way they identify potential persons-of-interest, collect usable intelligence, and conduct threat assessments.

In that case, how can individuals with malicious intent be identified in advance? How are they using the internet and social media to further their nefarious deeds? These questions can be addressed by examining how open-source digital footprints (i.e., one's online behaviours on social media and internet) should be harnessed to better identify and assess potential security threats. It is within these digital footprints where a potential perpetrator's intention and warning signs may manifest (Augenstein, 2017; Neo et al., 2017), which in turn can be utilised to assess the threat they pose. This chapter will discuss how digital footprints can be leveraged to identify potential security threats, particularly for crime and security issues that will result in negative repercussion at the national level, such as acts of violent extremism and hate crimes.

IDENTIFYING INDIVIDUALS WITH MALICIOUS INTENT USING THEIR DIGITAL FOOTPRINTS

The ability to disseminate information instantaneously and globally at very low costs provides these individuals with great opportunities to further their nefarious deeds. For example, on 29 October 2013, a video was released by an individual claiming to represent Anonymous via YouTube. It was addressed to the government of Singapore; the person threatened to disrupt key infrastructure in Singapore in an attempt to protest against the government's online regulatory framework (Neo et al., 2013). In another illustration, the Islamic State of Iraq and Syria (ISIS) spokesperson, Abu Mohammed al-Adnani, issued a call for attack on the 'enemies' of ISIS in 2014 via ISIS' repertoire of online platforms (Goh, Tan, Neo, & Khader, 2017). This led to an increase in the number of lone-wolf attacks by followers of ISIS in many parts of the world (Tee, Neo, Chin, & Khader, 2018). It is essential to note that such attempts to reach out and gain attention amongst the population would not have been possible without the internet. The internet has provided these individuals with a readymade audience to exert their influence and presence.

The use of information and communications technology inevitably leave behind publicly accessible digital footprints for intelligence and law enforcement agencies to follow. Personal information and stories (e.g., online expressions of personal sentiment, photographs of local places and happenings, geo-tagging a post, publicised social networks) are becoming easily available on websites and social media platforms (Whitty, Doodson, Creese, & Hodges, 2017). These changes in the access to digital footprints might be particularly useful for law enforcement and intelligence agencies who are increasingly drawing from online sources to assist in identifying potential security threats.

While this repertoire of open-source, highly personal and detailed cyber information can serve as leads for more technical means of intelligence gathering, the massive amount of these open-source digital footprints requires security agencies to be able to prioritise and focus their limited resources in their intelligence gathering endeavour (Skillicorn, 2009). There is also the need to ensure that the data points are reliable and credible. In the context of violent extremism, for instance, law enforcement agencies have utilised social media postings to incriminate individuals who are being radicalised online. In one case, Bilal Abood was arrested in Texas as a result of his Twitter activities. He used his Twitter account to pledge 'obedience' to ISIS leader, Abu Bakr al-Baghdadi, and had plans to travel to Syria to fight against the government of Bashar al-Assad. Although Abood originally denied that he had made the

Table 1. Eight warning behaviours

Warning Behaviours	Description
Pathway	Indication of research, planning and preparation of an attack
Fixation	Increasing preoccupation with person or cause
Identification	Identify with law enforcement, military paraphernalia, attackers or assassin
Novel aggression	Act of violence committed (unrelated to target) for the first time
Energy burst	Increase in frequency/variety of behaviours related to target
Leakage	Communication to a third party of an intent to do harm to the target
Last resort	Behavioural or verbal evidence of increasing desperation and distress
Directly communicated	Communication of a direct threat to target/law enforcement

pledge of allegiance to al-Baghdadi and ISIS, the particular post which identified this undertaking had in fact been ‘re-tweeted by others’ (United States of America v. Bilal Abood, 2015).

Consequently, the idea of leveraging digital footprints to detect potential security concerns is premised on the concept of assessing one’s online characteristics and attributes, to identify and decipher individuals with malicious intention. This may aid security agencies in identifying individuals who are at risk of orchestrating violent extremist attack, cyber-attacks, as well as hate crimes. The effectiveness of leveraging digital footprints, however, would require more than just its physical implementation of software and hardware (e.g., creating algorithms to identify relevant information) to support current operational practices. Besides understanding the mind and behaviour of the perpetrators, there is also about predicting and managing the identifiable behaviour effectively (Khader, Neo, Tan, Cheong, & Chin, 2019). As Khader (2011, pp. 5–6) opined, “behavioural sciences have much to say that should inform strategies for counterterrorism and counter-intelligence ... officers need to be constantly ahead of these behavioural trends by understanding through research the psyche of individuals, groups and trends”. The appreciation of how the field of behavioural sciences can act as force multipliers to understand perpetrators’ behaviours and cognitions will give us greater confidence on the steps that are required to search and identify potential security concerns in advance.

This chapter henceforth proposes the utilisation of insights from the behavioural sciences perspective to buttress the use of digital footprints: (i) identifying online warning signs; (ii) deciphering beliefs and motivations from social media data; and (iii) exploring the role of the online community.

Identifying Online Warning Behaviours to Targeted Violence

In the field of threat assessment, researchers have argued that there is always a pathway to targeted violence, with a series of perceptible thoughts and actions manifesting at each stage of the pathway (Borum, Fein, Vossekuil, & Berglund, 1999; Chai, 2019). The perpetrator’s actions would be influenced by a unique combination of precipitating characteristics and motivations over a period of time. To identify these perpetrators in advance, researchers have identified eight types of warning behaviours in the preceding days and weeks before they carry out their plans (Meloy, Hoffmann, Guldemann, & James, 2012; Meloy, Roshdi, Glaz-Ocik, & Hoffmann, 2015). Table 1 describes these eight warning behaviours by Meloy and colleagues (2012).

These warning behaviours are changes in behaviours that indicate an enhanced risk of violence which requires the relevant authorities to step in (Chai, 2019; Neo, 2018). However, the endeavour of assessing potential security threats is only possible if these warning behaviours are observed in the first place (Unsgaard & Meloy, 2011). Intelligence and information gathering are therefore crucial in detecting these warning behaviours. Extant research appears to suggest that out of these eight warning behaviours, some of them can be identified in the cyber realm. For instance, the warning behaviours of ‘leakage’, ‘fixation’, and ‘identification’ have been identified by Cohen and colleagues (2014) as having the highest likelihood of being exhibited by violent extremists in their online interactions within the group and their followers.

Leakage Warning Behaviours

Leakage warning behaviours refer to any expression of an intention to commit violent acts to a third party. Such online exchanges usually contain words that signal intent together with words that infer a preoccupation with the use of violence. This was seen in the ‘Unite the right’ rally by far-right followers, who are deemed as hate crimes perpetrators (Sheffield, 2017). On August 12, 2017, many far-right groups gathered to protest against the removal of the statue of a confederate general, Robert E. Lee in Charlottesville, Virginia. Violence broke out during the rally, resulting in three deaths. While attention has been focused on the violence perpetrated in the real-world, it is important to understand how these far-right groups used the internet to organise this rally. Based on leaked screenshot of chats from the app, Discord, these digital footprints showed participants planning for violence, expressing hatred and coordinating event logistics before the rally (Tiku, 2017). Through the leaked Discord chats, it was found that the perpetrators disguised a GoFundMe Campaign to raise funds for people to travel to Charlottesville so that they could attend the rally (Lecher, 2017).

Before conducting the 2019 Christchurch Mosque shootings, the perpetrator, Brenton Tarrant had posted on 8chan (i.e., an anonymous message board which allowed users to post radical right-wing thought) about his intentions to conduct an attack: “Well lads, it’s time to stop shitposting and time to make a real life effort post. I will carry out and attack against the invaders, and will even live stream the attack via facebook. The facebook link is below, by the time you read this I should be going live” (Resilience, Safety, and Security Psychology Branch, 2019, p. 3). Tarrant used Facebook to declare that he would be doing a live-stream video, and published his 74-page manifesto (Wakefield, 2019). The manifesto was sent to 30 New Zealand parliamentary email addresses (which included New Zealand Prime Minister Jacinda Ardern), and uploaded on social media nine minutes before the attack took place (Chavez & Holcombe, 2019).

Fixation Warning Behaviours

Fixation warning behaviours refer to any expression which signals an increasing pathological preoccupation with an ideology or person who is considered responsible for the individual’s grievance. For the former, some online users may express an ‘allegiance’, via their likes and associations, to a political party or radical movement that is deemed as sympathetic to their cause (Lucas & Aly, 2015). In the case of ISIS foreign fighters, they have publicly displayed their allegiance to the group, “We are no longer The islamic state of iraq and sham. We are only the ‘ISLAMIC STATE’. It’s official khilafa is restored! [sic]” (cited in Neo, 2018). For the latter, ISIS foreign fighters have demonstrated a strong preoccupation with groups that they deemed are responsible for the injustice faced by Muslims, “What treaty?? Didn’t America invade our lands rape our women torture us and kill our children, what treaty are u talking

about [sic]” (cited in Neo, 2018). There is an increasingly negative characterisation (e.g., anger, hatred) about the object of fixation in their digital footprints.

Identification Warning Behaviours

Identification warning behaviours refer to any narcissistic and grandiose online descriptions that indicate a desire to be a saviour or hero. The online users may espouse a warrior mentality, closely associate with weapons, and identify with a radical role model, group or radical action. Sympathisers and members of violent extremist groups often express an identification with radical leaders (military, ideological) or figures that are well known to be influential in any violent extremist groups or movements (Neo, Dillon, & Tan, 2016; Singh, 2011). For example, the social media pages of Anjem Choudhury, Musa Cerantonio, Ahmad Musa Jibril, and Anwar Al-Awlaki were some of the most common pages amongst ISIS supporters (Carter, Maher, & Neumann, 2014).

The capability to detect these three types of warning behaviours from one’s digital footprints—that are indicative of their intentions, ideology, and tactics—can serve as clues for intelligence and law enforcement agencies when conducting intelligence probes. This information is critical in aiding security agencies to identify and assess individuals who are potential security threats. More importantly, there is also some utility in carrying out further research to examine how these warning behaviours can be extrapolated to other online-related security threats.

Deciphering Beliefs and Motivations From Social Media Data

Information found on social media sites has become a valuable source of open-source data that could assist in the authentication and identification of an individual (Back et al., 2010; Whitty et al., 2017). A number of studies have attempted to use these digital footprints to predict an individual’s personality attributes—i.e., beliefs, motivations—, online behaviours, and feelings (e.g., Golbeck, Robles, & Turner, 2011; Quercia, Kosinski, Stillwell, & Crowcroft, 2011). For example, social media postings have been used to decipher an individual’s preferences for musical genres (Nave et al., 2018), employers’ hiring decisions (Newness, Steinert, & Viswesvaran, 2012), and likelihood of an individual having antisocial personality traits (Sumner, Byers, Boochever, & Park, 2012). A highly influential study by Kosinskia, Stillwell, and Graepel (2013) suggested that social media analysis can also offer a window into a broad range of characteristics including propensity for recreational drug use, status of parents’ marriage, preference for certain sports and teams, and political and religious views.

Recognising how online generated content by social media users may advance a deeper understanding of their beliefs and motivations, it can also be used to profile those that are of potential security concerns (e.g., radical worldviews, motivated by grievances). Such information could then be channelled towards the identification of relevant data point for intelligence and information-gathering. Within the field of online radicalisation, Edwards and Gribbon (2013, p. 45) argued that “[radical views] depends on the individual consumer in question ... while the internet might make information easier to find, ultimately the effect on the individual and their subsequent decision to take action will be a personal one”. In other words, what is of interest is how an individual’s characteristics (i.e., beliefs, motivation) can be used to assess an individual’s likelihood of becoming involved in violent extremism online. There is value to focus on personality dimensions like beliefs, motivations, as well as behaviours, where social media postings could be collected for data mining analyses to profile individuals of concerns in real time. For example, a set of personality, psycho-social and protective factors was identified by Neo (2018)

to detect individuals who might be involved in violent extremism online. In particular, six personality factors of interest were derived: perceived grievances; intolerance towards multi-religious, multi-racial living; knowledge to commit violent extremist offences; redemption and the pursuit for significance; susceptible to influence; and readiness to use violence. The author further validated these factors by comparing ISIS foreign fighters with ISIS sympathisers based on their social media postings on Twitter. It was revealed that the factor 'readiness to use violence' can be used to distinguish the foreign fighters from the sympathisers (Neo, Khader, & Pang, 2017). Beliefs as well as motivations of concern could be discerned from social media data by intelligence and law enforcement agencies when conducting intelligence probes. Furthermore, there is value to conduct further research to examine how other types online-related security threats could be informed by personality insights derived from social media data. However, the recent Cambridge Analytica scandal forces researchers and practitioners alike to reconsider the ethical concerns of harvesting personal data from social media users (Watkin, 2019).

Exploring the Role of the Online Community

While it is tempting to focus on the role played by personality-related factors and their functionality as predictors for online security threats, Pang (2016, p. 110) argues that "a practitioner who is seeking to use personality research to predict behavioural outcomes would not only need to know the type of behaviour a personality trait predicts, but also the specific environmental condition that is most likely to cause the behaviour to manifest". Since cyber-environments evolve more rapidly than physical environments, it is particularly important to contextualise the interaction of the individual, his/her current circumstances, and the influence of the online community to the process of identifying potential security threats.

Different threat actors would ascribe different meaning to their online behaviours based on these interactions. The internet has been exploited by violent extremists to create social milieus and subculture that cultivate partisanships and a community of like-minded individuals. This notion of an online community has been underscored by Bowman-Grieve (2009) when she observed that members in 'Stormfront', a radical right-wing forum, perceived themselves as part of a global community united by ties of solidarity that transcends geographical boundaries. For Tarrant, the Christchurch shooter, his online manifesto was able to inspire John Earnest to carry out a shooting in a synagogue in San Diego, Patrick Crusius to kill 21 people in a WalMart in El Paso, and Philip Manshaus to carry out a shooting in a mosque in Norway (Burke, 2019). While there was no evidence of direct cooperation between these attackers, there is a sense that they each feed off the other's narrative (Ward, 2019). Two of the attackers explicitly mentioned that Tarrant was a catalyst for their actions. They copied each other's ideas and formed a loose format for their atrocities, incorporating online manifestos, livestreams and memes from dark internet culture (Dearden, 2019). According to experts, members of these large right-wing online networks inspire and challenge each other to beat each other's body counts (Ward, 2019).

Furthermore, Hussain and Saltman (2014) suggest that the online violent extremist community can act as a replacement for the social environments that the members may lack in the real world. In this context, the internet does not only serve as an effective tool of communication, but also as an indirect medium to garner support and influence adherents' socialisation towards involvement in violent extremism. The endorsement of the radical ideology espoused by the online community may provide the 'push' factor that increases the likelihood of an individual to act in line with the ideology (Neo et al., 2017). It is within these online social interactions where an individual's motivation, intentions, and behaviours may ignite, and in the process, become potential security threats. Even in cases of lone-wolf attacks, these

perpetrators rarely become radicalised in complete isolation as they usually would have had engaged in some form of interactions with others in the online communities (Cohen, 2012).

It also suggests that it is important to focus not just on analysing the online violent extremist content, but also exploring how individuals use the internet to support violent extremist groups or movements. The structure and composition of an individual's online community may influence the course of action he/she might take (Ackland, 2013; Bartlett & Miller, 2013).

Using Social Media Analytics to Examine the Influence of the Online Community

Progress to identify potential online security threats can be made by understanding the online communities (e.g., social media platforms, websites, forums) and the dynamics within them. In her review of social media analytics, Yang (2016) described how tools can be developed to (i) map and measure the online social network, (ii) analyse online sentiment to identify which social media accounts to monitor, and (iii) examine the strength of relationships within the online communities. The outcomes of such analyses can help intelligence and law enforcement agencies explain the relationship between individuals (e.g., who is in their friend list, what is their membership status, their level of activity in the online community), and possibly predict behaviour resulting from these ties and even forecast potential security concerns. These online social networks may be explicit (i.e., memberships are formalised such as Facebook communities) or implicit (i.e., memberships are inferred based on online behaviours such as likes, comments, and links) in nature (Bartlett & Miller, 2013). These insights can then serve as a basis for understanding how close each individual is to the other individuals. For instance, social media analytics have been used to intervene in violent extremist financing networks, map networks of violent extremist organisations, and discover the role of each member of the online community (Barabási, 2012).

Researchers have attempted to utilise behavioural sciences and computational informatics methods to trace individuals with high risk of being radicalised by measuring 'signs and characteristics' from their interactions in online social networks (RiskTrack software tool; Camacho, Gilpérez-López, Gonzalez-Pardo, Ortigosa, & Urruela, 2016). The advantages of such a system is that it could guide the collection of digital footprints to track individuals of interest in real-time. Insights gleaned from the role of the online community can serve as valuable data points appropriate for cyber threat assessment. Future areas of research can focus on the manner in which other types of cyber actors with malicious intent may congregate online and influence one another.

SOLUTIONS AND RECOMMENDATIONS

In the current digital age, an assessment of security threats cannot be determined without looking at social media and online activity. These digital footprints offer intelligence and law enforcement agencies an alternative source of rich and potentially useful data (Antonius & Rich, 2013). Given that intelligence and law enforcement agencies have finite investigative resources (Skillicorn, 2009), the ability to analyse digital footprints would be crucial to better our understanding of online behaviour—particularly for crime and security issues such as violent extremism and hate crimes.

Solely depending on technological advancement to identify potential online security threats, would be insufficient in the long run (Yang, 2016). Amidst an increasingly complex operating landscape, it is essential to recognise how insights from a behavioural sciences perspective can enhance existing avail-

able measures or guide the development of new cyber-focused approaches. Hence, this chapter examines how three areas of behavioural sciences research (i.e., identifying online warning signs; deciphering beliefs and motivations from social media footprints; exploring the role of the online community) can help intelligence and law enforcement agencies who are seeking to leverage on the advantages of digital footprints to better identify online potential security threats.

Several implications for intelligence and law enforcement agencies are proposed. Firstly, to develop cyber threat assessment tools to complement offline information gathering. Some initial efforts can be seen in the development of CYBERA (see Pressman & Ivan, 2016), which analyses and assesses individual cyber-behaviour in support of violent extremism. The use of digital footprints to assess for threat also means that intelligence and law enforcement officers would have to be trained in new analytical skillsets so that the curated digital data can be properly analysed (Abdul Rahman, 2019). Related assessment tools can also be developed to analyse other types of cyber-related concerns such as insider threats, hate crimes, espionage, etc.

Secondly, to develop automated screening tools to detect individuals of concern based on their digital footprints. One of the most obvious implication arising from the discussion on the three areas of research is the manner in which a multidisciplinary approach (e.g., incorporating computational informatics methodology with insights from the behavioural sciences perspective) can be adopted to identify individuals with malicious intent. For example, behavioural sciences researchers can collaborate with computer scientists to employ machine learning (ML) and Natural Language Processing (NLP) technology to identify radical content on the internet. For instance, Gaydhani, Doma, Kendre, and Bhagwat (2018) used ML to automatically classify tweets on Twitter into three classes: hateful, offensive, and clean. The authors achieved an accuracy rate of 95.6 percent upon evaluating it on test data. Similarly, other researchers such as Biere (2018), have attempted to use principles of NLP to extract meaning from online postings and decipher their sentiments, in order to detect hate speech. Such techniques are especially useful given the large amount of data that is being uploaded onto the internet.

Thirdly, to work with social media companies to ‘adjust’ their recommendation algorithm with regards to radical content. Durkee (2019) reported that YouTube has modified its recommendation algorithm to limit recommendations of ‘borderline content and harmful misinformation’ that doesn’t violate YouTube’s rules outright. This ensures that the influence and outreach of such hate rhetoric are reduced. Further collaboration with social media companies should include the removal of radical content disseminated by individuals of concern, or remove or block social media accounts and websites that are perpetuating the radical ideology. However, it is important to note that ‘take down’ of radical content does not remove the perpetrators, it merely ‘displaces’ them and they may turn to other online platforms to disseminate their radical rhetoric.

Fourthly, to appreciate how the insights identified in this chapter could be utilised to guide the development of evidence-based research for various types of cyber threats such as scams, hacking, etc. Currently, this chapter largely focuses on how digital footprints can be leveraged to identify individuals who may endorse and engage in violent extremism. Thus, learning lessons can be extrapolated to help determine the types of data and information that are most useful for developing usable intelligence to prevent other types of cyber threats from materialising.

Fifthly, to identify the ‘right questions’ to guide the process of searching for relevant and useful digital footprints. Some challenges faced by security agencies may include: (i) the ambiguity in the meaning of the online behaviours attributed to the threats faced—they can vary from person to person; and (ii) the reliability and availability of data—it depends on the actions and choices of the users, social networking firms, as well as privacy regulations. In the event that a ‘wrong question’ is identified, it may lead

security agencies to overlook certain signals and focus their resources on data that form misleading or flawed assumptions about their person-of-interest.

Next, to advance the field of threat assessment in the local context. Whilst this might sound like a common-sense solution, there are not many local-based studies on cyber threat assessment. Notably, much of the emerging research on threat assessment (e.g., Meloy et al., 2012) were carried out in Western countries based on Western samples. Much more is still needed to address this paucity of local research, and ‘grow’ this business of threat assessment for online related security concerns. One difficulty of doing this kind of work well is that it requires a multidisciplinary approach. It requires a blended expertise on behavioural sciences (e.g., psychology, sociology, cultural studies, communication sciences), information and communications technology (e.g., machine learning, neural networks), and the use of empirical primary data to validate the process of threat assessment. Thus, some possibilities for future research questions include: (i) can threat assessment be done for other local cyber-related threats besides violent extremism? (ii) can insights from law enforcement databases be used to guide the research on threat assessment? and (iii) how can researchers better understand the interaction between personality characteristics of the individual and the online environment for these local cyber-related threats?

Lastly, it is important to introduce interventions that can directly mitigate the threat posed by individuals who have malicious intention. The act of assessment is not sufficient if there are no follow-up initiatives. In the content of combating online hate speech, efforts can be made to train community leaders and counsellors to engage with individuals of concern online about their hate rhetoric. This is to empower them with the knowledge and communication techniques so that they may engage those responsible for propagating hate speech. For example, as part of the ‘No Hate Speech Movement’, the Council of Europe conducted a series of training for young people to build their competences to combat hate speech on and offline (Council of Europe, 2016). Similarly, recognising the key role that the community can play in fighting hate and standing up to promote tolerance and inclusion, the Southern poverty Law Center (2017) has identified ten principles that members of the community can adopt to fight hate: (i) act; (ii) join force; (iii) support the victims; (iv) speak up; (v) educate yourself; (vi) create an alternative; (vii) pressure leaders; (viii) stay engaged; (ix) teach acceptance; and (x) dig deeper.

To conclude, the three areas of behavioural sciences research highlighted in this chapter may provide a basis for future research in helping intelligence and law enforcement agencies identify and predict potential security threats.

REFERENCES

- Abdul Rahman, M. F. (2019). Leveraging smart technology for better counter-terrorism intelligence. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 73–97). Singapore: World Scientific Press.
- Ackland, R. (2013). *Web social science: Concepts, data and tools for social scientists in the digital age*. London: Sage Publications.
- Antonius, N., & Rich, L. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The International Technology Management Review*, 3(1), 42–53. doi:10.2991/itmr.2013.3.1.4

Augenstein, S. (2017). NYC truck terror attack: New 'lone wolf' study may help analysis. *PoliceOne News*. Retrieved from <https://www.policeone.com/investigations/articles/455533006-NYC-truck-terrorattack-New-lone-wolf-study-may-help-analysis/>

Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B., & Gosling, S. D. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological Science*, 21(3), 372–374. doi:10.1177/0956797609360756 PMID:20424071

Barabási, A. (2012). *Network science*. Boston, MA: Barabási Lab.

Bartlett, J., & Miller, C. (2013). *The state of the art: A literature review of social media intelligence capabilities for counter-terrorism*. London: DEMOS.

Biere, S. (2018). *Hate speech detection using natural language processing techniques*. Vrije Universiteit Amsterdam. Retrieved from https://beta.vu.nl/nl/Images/werkstuk-biere_tcm235-893877.pdf

Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach to evaluating risk of targeted violence. *Behavioral Sciences & the Law*, 17(3), 323–337. doi:10.1002/(SICI)1099-0798(199907/09)17:3<323::AID-BSL349>3.0.CO;2-G PMID:10481132

Bowman-Grieve, L. (2009). Exploring “Stormfront”: A virtual community of radical right. *Studies in Conflict and Terrorism*, 32(11), 989–1007. doi:10.1080/10576100903259951

Burke, J. (2019, August 11). Norway mosque attack suspect ‘inspired by Christchurch and El Paso shootings’. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2019/aug/11/norway-mosque-attack-suspect-may-have-been-inspired-by-christchurch-and-el-paso-shootings>

Camacho, D., Gilpérez-López, I., Gonzalez-Pardo, A., Ortigosa, A., & Urruela, C. (2016, November). *CEUR Workshop Proceedings*. Retrieved from <http://ceur-ws.org/Vol-1794/afcai16-paper5.pdf>

Carter, J. A., Maher, S., & Neumann, P. R. (2014). *Greenbirds: Measuring importance and influence in Syrian Foreign fighter networks*. London: ICSR.

Chai, W. (2019). Threat assessment of violent extremism: Considerations and applications. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 53–72). Singapore: World Scientific Press.

Chavez, N., & Holcombe, M. (2019, March 17). Death toll rises to 50 in New Zealand mosque shootings. *CNN*. Retrieved from <https://edition.cnn.com/2019/03/16/asia/christchurch-new-zealand-mosque-shooting-latest/index.html>

Chen, X., Tan, J., Goh, P., Ong, G., & Khader, M. (2018). *Frequently asked questions about fake news* (HTBSC Research Report S02/2018). Singapore: Home Team Behavioural Sciences Centre.

Cohen, K. (2012). Who will be a lone wolf terrorist? Mechanisms of self-radicalisation and the possibility of detecting lone offender threats on the internet. Swedish Defence Research Agency (FOI).

Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting linguistic markers for radical violence in social media. *Terrorism and Political Violence*, 26(1), 246–256. doi:10.1080/09546553.2014.849948

Conway, M. (2007). Terrorist use of the Internet and the challenges of governing cyberspace. In D., Myriam, V., Mauer, & F., Krishna-Hensel (Eds.), *Power and security in the information age: Investigating the role of the state in cyberspace* (pp. 95-127). London: Ashgate.

Council of Europe. (2016). *Training seminar countering hate speech through human rights education and narratives*. Retrieved from <https://rm.coe.int/16806efc97>

Dearden, L. (2019, August 25). Revered as a saint by online extremists, how Christchurch shooter inspired copycat terrorists around the world. *Independent*. Retrieved from <https://www.independent.co.uk/news/world/australasia/brenton-tarrant-christchurch-shooter-attack-el-paso-norway-poway-a9076926.html>

Dillon, L. (2016). Cyberterrorism: Using the internet as a weapon of destruction. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 426-451). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch021

Durkee, A. (2019, June 5). YouTube is finally taking a harder line on hate speech. Is it too little, too late? *Hive*. Retrieved from <https://www.vanityfair.com/news/2019/06/youtube-hate-speech-too-little-too-late>

Edwards, C., & Gribbon, L. (2013). Pathways to violent extremism in the digital era. *The RUSI Journal*, 158(5), 40-47. doi:10.1080/03071847.2013.847714

Europol. (2014). *TE-SAT 2014. European Union terrorism situation and trend report 2014*. European Law Enforcement Agency.

Gan, R., Neo, L. S., Chin, J., & Khader, M. (2018). *The psychology of hate: A case study analysis of the 2018 Sri Lanka Kandy Riots (HTBSC Research Report 18/2018)*. Singapore: Home Team Behavioural Sciences Centre.

Gaydhani, A., Doma, V., Kendre, S., & Bhagwat, L. (2018). *Detecting Hate Speech and Offensive Language on Twitter using Machine Learning: An N-gram and TFIDF based Approach*. Retrieved from <https://arxiv.org/pdf/1809.08651.pdf>

Goh, P., Tan, J., Neo, L. S., & Khader, M. (2017). *Understanding crowd behaviour during violent extremist attacks: Insights from the Nice truck attack 2016 (HTBSC Research Report 16/2017)*. Singapore: Home Team Behavioural Sciences Centre.

Golbeck, J., Robles, C., & Turner, K. (2011). Predicting personality with social media. *Extended Abstracts on Human Factors in Computing Systems*, 253-262.

Hussain, G., & Saltman, E. M. (2014). *Jihad trending: A comprehensive analysis of online extremism and how to counter it*. London: Quilliam Foundation.

Khader, M. (2011). Behavioural sciences in Home Team operations: 'Mindware' to complement our hardware. *Home Team Journal*, 3, 4-9.

Khader, M., Neo, L. S., Tan, J., Cheong, D. D., & Chin, J. (2019). Learning from violent extremist attacks: An introduction. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 33-62). Singapore: World Scientific Press.

Kosinskia, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States*, 110(15), 5802–5805. doi:10.1073/pnas.1218772110 PMID:23479631

Lecher, C. (2017, August 30). Neo-Nazis disguised GoFundMe campaign as a ‘family reunion’ in Charlottesville. *The Verge*. Retrieved from <https://www.theverge.com/2017/8/30/16227142/gofundme-campaigns-charlottesville-unite-the-right>

Lucas, K., & Aly, A. (2015). Counter narratives to interrupt online radicalisation. A report on the CNOIR project presented to the Department of Attorney General. Australia: Countering online Violent Extremism Research Program, Curtin University.

Luo, X. S., & Wang, P. (2018). *(Up)skirting the law: An online perspective (HTBSC Research Report 12/2018)*. Singapore: Home Team Behavioural Sciences Centre.

Meloy, J. R., Hoffmann, J., Guldemann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30(3), 256–279. doi:10.1002/bsl.999 PMID:22556034

Meloy, J. R., Roshdi, K., Glaz-Ocik, J., & Hoffmann, J. (2015). Investigating the individual terrorist in Europe. *Journal of Threat Assessment and Management*, 2(3-4), 140–152. doi:10.1037/tam0000036

Nave, G., Minxha, J., Greenberg, D. M., Kosinski, M., Stillwell, D., & Rentfrow, J. (2018). Musical preferences predict personality: Evidence from active listening and facebook likes. *Psychological Science*, 29(7), 1145–1158; Advance online publication. doi:10.1177/0956797618761659 PMID:29587129

Neo, L. S. (2018). *Understanding personality, psychosocial, and protective predictors of online violent extremism. Paper submitted for PhD qualifying Examination and Conversion*. Singapore: Nanyang Technological University.

Neo, L. S., Dillon, L., & Khader, M. (2017). Identifying individuals at risk of being radicalised via the internet. *Security Journal*, 30(4), 1112–1133. doi:10.1057/1284-016-0080-z

Neo, L. S., Dillon, L., & Tan, J. (2016). *Violent extremist cyber footprints: A guide to understanding and countering online violent extremism* (Rev. ed). Singapore: Home Team Behavioural Sciences Centre.

Neo, L. S., Khader, M., & Pang, J. S. (2017). Comparing ISIS foreign fighters versus sympathiser: Insights from their Twitter postings. *Home Team Journal*, 7, 87–106.

Neo, L. S., Shi, P., Wang, Y., Wang, P., Khader, M., & Ong, G. (2013). *Defining Singapore’s “anonymous problem” (HTBSC brief research report S02/2013)*. Singapore: Home Team Behavioural Sciences Centre.

Newness, K., Steinert, J., & Viswesvaran, C. (2012). Effects of personality on social network disclosure: Do emotionally intelligent individuals post inappropriate content? *Psihologiske Teme*, 21(3), 473–486.

Pang, J. S. (2016). Understanding Personality and Person-specific Predictors of Cyber-based Insider Threat. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 107–128). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch006

Pressman, D. E., & Ivan, C. (2016). Internet use and violent extremism: A cyber-VERA risk assessment protocol. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 402–420). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch019

Quercia, D., Kosinski, M., Stillwell, D., & Crowcroft, J. (2011). Our Twitter profiles, Our selves: Predicting personality with Twitter. *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. 10.1109/PASSAT/SocialCom.2011.26

Resilience, Safety, and Security Psychology [RSSP] Branch. (2019). *6 big questions about the 'day after' Christchurch mosque shootings* (HTBSC Research Report 07/2019 [revised]). Singapore: Home Team Behavioural Sciences Centre.

Savage, C. (2013, February 28). Soldiers admits providing files to Wikileaks. *The New York Times*. Retrieved from <https://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html>

Sheffield, M. (2017, August 21). Big Tech, the alt-right and the unknown future of the internet. *Salon*. Retrieved from <http://www.salon.com/2017/08/21/big-tech-the-alt-right-and-the-unknown-future-of-the-internet/>

Singh, K. (2011). The 'Osama' of the internet: Anwar al-Awlaki. *Behavioural Insights*, 21.

Skillicorn, D. (2009). *Knowledge discovery for counterterrorism and law enforcement*. New York, NY: CRC Press.

Southern Poverty Law Center. (2017, August 14). *Ten ways to fight hate: A community response guide*. Retrieved from <https://www.splcenter.org/20170814/ten-ways-fight-hate-community-response-guide>

Sumner, C., Byers, A., Boochever, R., & Park, G. J. (2012). Predicting dark triad personality traits from Twitter usage and a linguistic analysis of Tweets. *Proceedings at the IEEE 11th International Conference on Machine Learning and Applications (ICMLA)*, 386–393. 10.1109/ICMLA.2012.218

Tan, C. W. T., & Wang, P. (2017). *The psychology of ransomware: Manipulation of human emotion for criminal activity* (HTBSC Research Report 02/2017). Singapore: Home Team Behavioural Sciences Centre.

Tee, S. H., Neo, L. S., Chin, J., & Khader, M. (2018). *Defeated but alive: The latent threat of ISIS* (HTBSC research report 16/2018). Singapore: Home Team Behavioural Sciences Centre.

Tiku, N. (2017, August 26). Alt-Right Chat Logs Are Key to Charlottesville Lawsuits. *Wired*. Retrieved from <https://www.wired.com/story/leaked-alt-right-chat-logs-are-key-to-charlottesville-lawsuits/>

United States of America v. Bilal Abood. (2015). *Indictment No. 3-15CR-0256K: In the United States District Court for the Northern Division of Texas Dallas Division-Filed June 10, 2015*. Retrieved from http://www.investigativeproject.org/documents/case_docs/2747.pdf

Unsgaard, E., & Meloy, J. R. (2011). The Assassination of the Swedish Minister for Foreign Affairs. *Journal of Forensic Sciences*, 56(2), 555–559. doi:10.1111/j.1556-4029.2010.01653.x PMID:21210810

Vishwanath, A. (2016). Spear phishing: The tip of the spear used by cyber terrorists. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 469–484). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch023

Wakefield, J. (2019, 16 march). Christchurch shootings: Social media races to stop attack footage. *BBC*. Retrieved from <https://www.bbc.com/news/technology-47583393>

Ward, A. (2019, August 12). A Norwegian white nationalist tried to kill Muslims at a mosque. *Vox*. Retrieved from <https://www.vox.com/2019/8/12/20801735/norway-mosque-attack-el-paso-muslims>

Watkin, W. (2019). *What we learned from Cambridge Analytica*. Retrieved from <https://www.brunel.ac.uk/news-and-events/news/articles/What-we-learned-from-Cambridge-Analytica>

Weimann, G. (2004). *How modern terrorism uses the Internet. Special Report No.116*. United States Institute of Peace. Retrieved from www.terror.net

Whitty, M. T., Doodson, J., Creese, S., & Hodges, D. (2017). A picture tells a thousand words: What Facebook and Twitter images convey about our personality. *Personality and Individual Differences*; Advance online publication. doi:10.1016/j.paid.2016.12.050

Yang, J. H. (2016). Social media analytics for intelligence and countering violent extremism. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 328–348). Hershey, PA: IGI Global.

ADDITIONAL READING

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict and Terrorism*, 40(1), 77–89. doi:10.1080/1057610X.2016.1157408

Meloy, J. R., Hoffmann, J., Guldemann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30(3), 256–279. doi:10.1002/bsl.999 PMID:22556034

Meloy, J. R., Roshdi, K., Glaz-Ocik, J., & Hoffmann, J. (2015). Investigating the individual terrorist in Europe. *Journal of Threat Assessment and Management*, 2(3-4), 140–152. doi:10.1037/tam0000036

Neo, L. S. (2016). An Internet-mediated Pathway for Online Radicalisation: RECRO. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 197–224). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch011

Pang, J. S. (2016). Understanding Personality and Person-specific Predictors of Cyber-based Insider Threat. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 107–128). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch006

Pressman, D. E., & Ivan, C. (2016). Internet use and violent extremism: A cyber-VERA risk assessment protocol. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 402–420). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch019

Saifudeen, O. A. (2014). *The cyber extremism orbital pathways model*. Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University.

Torok, R. (2013). Developing an explanatory model for the process of online radicalisation and terrorism. *Security Informatics*, 2(1), 1–10. doi:10.1186/2190-8532-2-6

KEY TERMS AND DEFINITIONS

Identification Warning Signs: Signs that showcase evidence of identifying with law enforcement, military paraphernalia, attackers, or assassin.

Leakage Warning Signs: Signs that showcase evidence of communication to a third party of an intent to do harm to the target.

Online Communication: Any kind of communication between either individuals or organisations that occurs on the internet.

Threat Assessment: Threat assessment is a structured group process used to evaluate the risk posed by a student or another person, typically as a response to an actual or perceived threat or concerning behaviour.

Violent Extremism: A willingness to use or support the use of violence to further particular beliefs, including those of a political, social, or ideological nature. This may include acts of terrorism.

Warning Signs: Warning signs are acts which constitute evidence of increasing or accelerating risk.

Investigating Cybercrime in Nigeria

Mufutau Temitayo Lamidi

University of Ibadan, Nigeria

INTRODUCTION

Information communication technology (ICT) is a means by which relevant online information is managed effectively to achieve desired results. It involves the use of various electronic gadgets such as computers (desktop and laptop), tablets, iPad and other phone types as tools to access, manage or handle different forms of information on the Internet and derive from it the advantages it offers. Given the several advantages of ICT to national development, Nigeria, among other countries, has keyed in into it to partake of the benefits ICT offers. With a population of 186,987,563, Nigeria's Internet penetration is estimated to be 52.02% (African Union Commission & Symantec, 2016: 81). The Internet is gaining popularity by the day as it gains adherents with more people using it for their various needs. However, the advances in ICT have been both a blessing and a curse to Nigerians. It has improved people's lives in different areas, ranging from information dissemination to social networking, advertising, marketing, Internet banking and money transfer, among others. It has made conducting businesses by some professionals, especially in banking and finance, journalism and entertainment sectors, more effective. Particularly, it has enhanced government's cashless policy, which discourages citizens from carrying huge cash around town whether for business transactions or to purchase commodities in markets. Despite its several advantages, it also has disadvantages, principally, in cyber-attacks. Nwogwugwu & Uzoechina (2015) observe that although crimes (especially economic crimes) predated globalization, globalization and ICT that have promoted Nigeria's economy globally have become useful tools in the hands of economic offenders to commit crimes and launder proceeds of their illicit acts.

Reports are rife in newspapers, online forums and blogs about incidents of cyber-attack in Nigeria. This study investigates different cyber-attacks which are usually subtle and felt largely by the generality of Nigerians. The aim is to examine its nature in order to offer advice towards stemming its tide.

BACKGROUND

Cybercrime is described as "crimes committed on the internet using the computer as either a tool or a targeted victim." (Kamini, 2011: 240). The computer is a tool when it is used against a victim such as in theft, pornography and online gambling; and the computer is a target when its programme, software or structure is deliberately destroyed/vandalised.

Cybercrime can be targeted at organisations, individuals or the society at large. For organisations, governments, firms, companies or groups of individuals are usually targets. In this wise, there is unauthorised access to/control of computer system, possession of unauthorised information, cyber terrorism against government organisation and distribution of pirated software (Kamini, 2011). For instance, Symantec (2016: 81-82) reports that Nigeria has faced a daily increasing challenge in vulnerability User Datagram Protocols, UDP, up to 25%; botnet drones, 20%; web defacement of government websites, 3%

DOI: 10.4018/978-1-5225-9715-5.ch069

increase, weekly average; and phishing, 4% daily average. Hence, it is no surprise that Nigeria has ranked third in four consecutive years (2006, 2007, 2008 and 2009) on the list of world cybercrime perpetrator countries (Dagaci et al., 2014).

For individuals, their person or property is the target. Individuals often get harassed through e-mail, cyber stalking, dissemination of obscene materials, defamation, indecent exposure, e-mail spoofing, cheating and fraud. Their properties may be vandalised, viruses may be introduced into their systems, and there may also be intellectual property thefts, Netrespass Internet time theft and unauthorised control/access over their computer systems.

For the society at large, cybercriminals target anyone and everyone indiscriminately. In this category are cybercrimes such as (child) pornography, polluting the youth through indecent exposure, trafficking, financial crimes, sale of illegal articles, online gambling and forgery.

Cybercrime has been studied from different perspectives. Studies such as Ayofe and Osunade (2009) and Dagaci et al. (2014) view Cybercrime from a generalist point of view. Kamini (2011) and Toyo (2017) actually investigated it as a phenomenon, especially in their country or state of abode, and Aribake (2015) and Ojeka et al. (2017) studied it from a professional angle. In addition, while Okeshola & Adeta (2013) and Omodunbi et al. (2016) studied cybercrime from a sociological perspective, Nwogwugwu & Uzoechina (2015) looked at it from an economic perspective, Chawki (2009) from a legal perspective, and Boniface & Michael (2014) from a technological perspective.

Against the backdrop of Nigeria being ranked third on the list of world cybercrime perpetrator countries for four consecutive years, Dagaci et al. (2014) examine the major causes, forms, rate of victim, economic cost to Nigeria and alternative strategies of reducing the menace. Ayofe and Osunade (2009) also define the concept of cybercrime and identify reasons for it, how it can be eradicated, those involved and the reasons for involvement. They suggest how to detect criminal mails and proffer solutions to checking the increasing rate of cybercrimes and criminals.

Kamini (2011) is one of the studies that examine the effect of cybercrime in India. It discusses the types of cybercrime, the mode and manner of its application as well as the legal frame operating against cybercrime in India. It finally suggests what individuals and corporate bodies can do to prevent cyber-attack. Another study is Toyo (2017), which focuses on Abraka in Delta State of Nigeria. The study examines the causes and types of cybercrime prevalent in Abraka, the players and the impact on the society. It identifies causes of cybercrimes as urbanisation, quest for wealth, weak implementation of cybercrime laws and ill-equipped security agencies as well as negative role models. It observes that yahoo attack and hacking are the most prominent cybercrimes in Abraka; and cyber-attacks often result in financial losses, mistrust of youths, carnal abuse and government's abandonment of rural communities. It suggests some control measures like establishment of national institutions, awareness and training, upholding ethical and moral standards, using computer forensics and anti-virus, and establishment of laws to control the menace.

Okeshola & Adeta (2013) and Omodunbi et al. (2016) also discuss cybercrime from the perspective of education and society. The researchers drew data from tertiary institutions in Zaria and Ekiti State. They identified different reasons why cybercrime thrives and proffered suggestions to curb its menace. They noted that youths, especially males, are the major players in cybercrime. Okeshola & Adeta, for instance, identified some of the motivational factors as

...money/ financial gain, recognition/fame, low rate of conviction or even being caught, easy to perpetrate, intellectual pursuit, frustration, revenge, display of wealth by corrupt politicians and yahoo yahoo boys, laziness, un satisfaction(sic) from what they earn, lack of good moral upbringing from parents and guardians (p. 110).

Another researcher, Chawki (2009), discusses the laws guiding the crime of Advance Free Fraud as well as how effective it is in the context of cybercrime. The study suggests that the laws against cybercrime be strengthened and security officers and legislature be trained in the application of laws to arrest the menace. Boniface & Michael (2014) on the other hand suggest that Internet technology be improved such that each internet user will be identifiable through their identification details which must have been pre-registered prior to their use of the Internet.

These studies provide a background for the current paper. Being a developing country that is still struggling to combat Cybercrime, Nigeria may compare notes with India, given the author's submissions as regards what India has achieved so far regarding the control of cybercrime. Toyo (2017), Okeshola & Adeta (2013) and Omodunbi et al. (2016) are also relevant as they provide instances of what happens in selected places in the three major regions of Nigeria. Unlike them, however, the current paper is not restricted to a particular region in Nigeria but focuses only on individual and societal cyber-attacks.

Two of the studies being discussed here concentrate on the professional aspects where the negative impact of cybercrime is felt. These are Aribake (2015) and Ojeka et al. (2017). Aribake (2015) examines the effect of ICT tools in curbing cybercrime in Nigerian commercial banks. According to the study, ICT in banks has both advantages and disadvantages. It enables competition among banks for the optimum delivery of services. However, the major snag is security, in which case, depositors' confidential information is at risk of abuse by criminals. This is a great challenge to Nigerian banks and their customers. Although Nigerian banks use different facilities to protect their businesses from fraudsters, these have very little effect and make online banking difficult and intricate. Hence, economic fraud and internet scams, among others, are manifest. Worse still is the insufficiency of electricity and telecommunication facilities, which consequently limit the improvement of online banking in Nigeria. Nevertheless, there has been a stupendous growth in the use of phones in Nigeria; but this has also facilitated an increase in cybercrime in the country. The study concludes that cybercrime is difficult to combat due to its complex nature and suggests the use of 'a unified and synchronized tactic encouraged by dynamic ICT security system' (p6). The study canvasses the preparation of a cyber-activities guideline to protect bank customers' interests.

In the same vein, Ojeka et al. (2017) examine the nature and dynamics of cybercrime and its contribution to the socio-economic development challenges in Nigeria. Anchored on Risk Theory, the study observes that the Internet revolution and the advent of mobile phone technology in Nigeria have posed unintended challenges to the country. It argues that widespread cybercrime in Nigeria tarnishes the country's image, discourages foreign investment, and reduces people's confidence in digital economy. Hence, it recommends the inclusion of security experts among audit panels, the establishment of laws and capacity building of security experts on contemporary cyber technology. Okeshola & Adeta (2013) also recommend training law enforcement agents while Chawki (2009) suggests strengthening the law against cybercrime and Boniface & Michael (2014) recommends technological innovation to identify internet users.

These studies are also relevant to the current study in that they discuss different forms of cybercrime in Nigeria which the current study is examining from different personal and social perspectives. The focus of this study is on individual and social cyber-attacks.

FOCUS OF THE ARTICLE

Data collection was in two categories. The first category of data was sourced from recalled personal experiences of attempted attacks (through phone calls, text messages and Facebook) on the researcher. The second category of data came from reports by individuals on social media such as WhatsApp, Twitter, Facebook and Nairaland Forums, some online newspapers (*Premium Times*, *National Helm* and *Pulse*) and a blog (www.ladiesgist.com). While Facebook and Twitter are online forums with members from across the globe, the WhatsApp platform and Nairaland Forum are populated principally by Nigerians. Nevertheless, there is a handful of non-Nigerian participants on Nairaland. Stories are taken from the archives of these online sources for discussion and/or exemplification of cases. Data are analysed descriptively.

Fraudulent Phone Calls

Cell phones are very useful in communication. Instead of travelling several kilometres to get or deliver some information, one can easily use the phone to request or pass on information and avoid the stress of travelling or even accidents on the road. However, this facility has been abused by criminals. The first part of it is that a criminal may look for a potential victim's number and call him or her with a hidden/private number. The criminal could then address the receiver usually by their first name or any name that people usually call them. Then, he (in my experience, the callers have always been males) would encourage the receiver to take a guess as to who their caller 'friend' was in Britain, America or such other fanciful places. The naïve receiver may mention a name, and pronto, the con man will latch on to it. He would exchange banter with the receiver briefly before stating 'the business offer' that prompted him to call. It may be a supply of goods to an agency or some kind of contract. If the receiver shows eagerness, the caller will ask him to call him back and hang up. In this process, the would-be victim may be asked to bring some initial deposit to facilitate the order and supply. This researcher has received up to five of such calls at different times. This fraudulent practice attempts to exploit the target's potential greed. If the target is greedy, they would be calculating the gains on the supply instead of the manner the business came about. In so doing, they fall into the trap and get duped.

A participant on Nairaland Forum also narrated his experience of attempted scam through phone about how a fraudster requested to buy property worth 7 million naira from him and the fraudster claimed he was ready to transfer the money to the seller without any prior contact on phone or physically. The second day, the fraudster changed his mind and said he would send the cash by road, but that it would be concealed inside a refrigerator. The day the money was expected, the seller got a call from a 'driver of the vehicle' ostensibly conveying the refrigerator that he had been stopped by the police at a checkpoint, and that the police were demanding N80,000.00 bribe before they would allow the vehicle to pass; otherwise they would open the content since they suspected that it was carrying ammunition for use by the Boko Haram insurgents. The seller who had seen through the deceit told them his phone data was exhausted and requested that he be sent a recharge PIN of N1000.00 to enable him to send the money to the account sent to him. The fraudsters realized that he had blown their cover and hailed him for being intelligent. The fraudsters played on the general belief that the police were corrupt. They expected that by using this trick, the victim would quickly send money to bribe the police, since the mount is far less than the 7 million naira he was supposedly going to earn. It follows that in all financial transactions, people must reason well before taking some decisions in order not to fall into such traps.

Another form of the use of phones is text messages. A message can be sent to a target bordering on certain issues in the society. While the communication networks in Nigeria were offering promotion services to subscribers, the researcher had got text messages from each of his MTN and Glo lines that he had won a million naira in each. He was assigned a serial number and asked to call a particular number to redeem his prize. When he called, the scammer told him that he must first buy a 48,000.00 naira worth of recharge cards and send to the scammer. When queried that it was supposed to be a prize which could have been transferred easily into the winner's account, the fraudster said the money the researcher was being requested to pay was for 'processing'. When told to take the money for processing from the winning, he said the prize would not be released until it was processed. The researcher went to report to his bank the second day and he was told they were fraudsters. If he had been eager to get the prize he neither participated in nor worked for, he would probably have fallen victim. Again, the fraudster is playing on the victim's intelligence, gullibility and, possibly, greed.

Another form of text messaging has to do with Bank Verification Number (BVN). Every account holder in banks in Nigeria is expected to have a BVN. This enables government to monitor cash flow in and out of customers' accounts. However, criminals often used this to collect information from account holders and subsequently steal their money. Fraudsters send text messages to account holders informing them that due to BVN problems, their accounts have been blocked and that the bank customers will not be able to use their Automated Teller Machine (ATM) cards any longer. To solve the problem, such bank customers are advised to call a number supplied in the text message. This is impersonation /identity theft in practice. Fraudsters assume the position of bank staff and request vital information such as Personal Identification Number (PIN) of ATM cards, BVN and other relevant resources that will enable them to get into people's accounts and fleece them of their money. To protect customers, however, banks often advise them not to divulge their secret/relevant information to third parties. In cases where bank customers are in doubt, they are to contact the bank. This kind of text message from fraudsters is playing on the intelligence of the bank customer. An unintelligent or careless customer may lose money through this scam.

Some other text messages can target positions. In a society where one lobbies and sometimes pays to get something, a naïve person would consider himself or herself lucky to have a message sent to him offering them a chance to be minister in a central government. Given the researcher's status as a university lecturer, some crooks sent him text messages that the presidency was considering him for a ministerial appointment. He was asked to send his CV to a mail and call a number. He did not. Sometimes later, he received a call conveying the same message; he rebuked the caller. Again, he got another text message on the same subject much later. The fact is: the researcher believed that if the presidency needed his services, he would get an official letter, not text messages. He probably escaped the hook because he knows the procedures such invitations should take; and especially because he was not eager to jump at offers, regardless of their worth. If he had acceded to their request to submit his CV, the fraudsters would probably have picked some new pieces of information to make money out of him.

Scam E-Mails

Fraudsters also explore the e-mail facility to dupe unsuspecting victims. A colleague travelled to Germany. Criminals hacked into his e-mail account and, posing as the lecturer, used it to send a message to his student in Nigeria that she should send some money into 'his uncle's account' on his behalf. When the student asked her supervisor, he denied ever sending such a message. In this case, the fraudster wanted to exploit the mutual respect that normally obtains between supervisor and student. If the student had not

been bold enough to find out the truth, she would have fallen victim. So, criminals also explore identity theft and our culture of respect to defraud citizens.

Criminals send spam mails to undisclosed recipients claiming that some money had been deducted from their accounts because of certain bank products they had purchased. Here are examples from my yahoo mail box:

1. Dear Customer,
 Thank you for successfully SUBSCRIBING For Diamond Mobile App bull monthly Bulletins.
 We are processing to debit your account with the sum of 20,5000 NGN as our monthly charge for the subscription as per ur terms and conditions.
 If you are not aware of this subscription and Wish to Cancel this, kindly follow our website link below to unsubscribe.
 Note: To unsubscribe, A mobile code will be sent to your registered mobile number to Cancel After Security Validation....
2. Dear Customer,
Your DiamondOnline (MOBILE BANKING) Account will be BLOCKED due to too many Login attempts. Kindly Click Here to RE-VALIDATE to avoid Account Suspension within Hours. A code will be sent to your registered mobile number with us, kindly fill in the code to complete the process.

These messages purport to come from the different banks stated in the mails. The snag is the researcher does not have any account with these banks. It is obviously the work of fraudsters who want to obtain relevant PIN numbers to cash away unsuspecting bank customers' moneys. A closer look at the messages show they have attempted to clone the banks message template. However, the informal language *as per* and cyber language *ur* (ex 1), multi-coloured graphics and the misapplied punctuation (especially on 20,5000) as well as the emphasised threats easily give away the fraud in the mails.

The researcher has also received several e-mails purporting to originate from distant lands such as Burkina Faso. The writer is usually a government official who had stolen some money and wanted 'us' to start a business with it in Nigeria, or a widow who lost her husband in gruesome circumstances but is now looking for a safe haven to invest her inherited money, or an orphan who inherited stupendous money. The writer would claim to trust the recipient such that they could do business together. The first indication that it was fake would be the problem of grammar or mechanics of language generally. The second aspect is the logic behind the set up: why would a total stranger trust completely someone she or he had never seen? These are the major considerations on why the researcher never bothered to pursue any of them. Another variant of this is the mail that requests friendship. The author of the mail, usually with a photograph of a beautiful lady may request friendship from the target victim. Again, this comes across as working on the usual weakness of some men. The researcher is not aware of anyone he knows who fell for this scam. However, the fact that it was rampant at a period suggests that some people did fall for it. Here is an example of such mails directed at people seeking love:

3. We are going to help you find sexy females between the ages of 19 and 25 that want to fuck!
 This is going to sound crazy, but it's the real thing.
4. They are eager to meet new men today. They are sick and tired of dating guys that cannot perform in the bedroom. [Come check their profiles here](#)

The eager juvenile may jump at this offer. If it turns out to be true, another juvenile is corrupted. A click on the link leads to pictures of stark-naked females. The questions on the page enquire whether one is up to 18, whether one is ready to abide by the condition that the women did not want any relationship, whether one agrees to use condom and whether one would not reveal the identities of familiar faces among the ladies. One has to click YES or NO on each question as a form of answer. However, whichever one clicks, one is still allowed to continue browsing! This means that the questions are just cosmetic; they serve to deceive new entrants into the world of prostitution or pornography.

Sometimes, the intent is not to immediately get money, but to get access to crucial information. Fraudsters may send mails to individuals that their mail accounts (such as yahoo) had to be closed down due to a request they had made. The account holder would then be advised to click a link to stop it if they did not want it closed. It would be emphasised that the account holder would lose all the contents of the mail box. Experience has shown that all the threats in this kind of mail never came to pass. No one deletes the account; one only falls into a trap if one proceeds to click on the link.

A scam mail can also be in form of a blackmail. The author may accuse the owner of the account of visiting some adult sites, quoting IP address of the target dupe's browser. The author may request that a specified amount of money be paid into his or her bank account, otherwise, pictures from such places visited by the addressee would be packaged and sent to all contacts in the person's mailing list. The idea is to blackmail that person into paying the criminal. The fact is that only the guilty may feel jittery; the innocent will not. The writer is playing on the possibility that the addressee will fall into the category of people that visit adult sites. Such people who may not want other people to know about their dirty secrets may quickly pay. However, they always forget, or do not know, that blackmailers never desist.

Cyber-Attack Through Leaked Video Messages/Pictures

There are several cases of leaked video messages and photographs. These are in different categories. The first category is that of husbands who caught their wives cheating. Video recordings of such cheating men and women are made and posted on the Internet. In another case, some secretly recorded videos of important personalities/celebrities and their partners are often released to the public to embarrass the target victims for whatever reason known to the poster. It may be for purposes of blackmail or a revenge if the victim is considered too powerful for the person that posted the video.

Sometimes, technicians who repair laptops, tablets and phones have also allegedly released nude pictures of their clients to the public through the Internet. They often claimed they stumbled on the pictures in the gadgets, but they have not confessed that they were blackmailing the owners of the videos. A university professor was once caught in the web¹. A female student of his got hold of his phone and asked him to send her huge sums of money. When the professor refused, his nude photographs were displayed on the Internet. The student's claim was that he had been sexually harassing her while she was taking his courses. The university administration set up a panel to look into the matter, but the complainant did not show up to defend her claim!² Some disgruntled boyfriends also released nude photographs of their former girlfriends to the public via the internet. Usually, this happens when the girlfriend dumps the boyfriend. These are acts of human rights abuse by individuals.

Nevertheless, some people deliberately post raunchy photographs of themselves on the web to attract people to their profiles. The females are usually nude or half nude, showing the curves of their body in the pictures. Some claimed to be looking for sex partners while others were just 'expressing themselves'. Some of the photos were taken in nudity by couples who had just made love; some by teenagers in undergarments. The problem with this is that it encourages immorality among children and adolescents

who may stumble on such posts, thus debasing our cultural values. Although the intent is different, it is mild pornography which may fascinate children and encourage them to practise same. It has a corrupting influence on children, encouraging moral depravity.

Cyber-Attack Through WhatsApp Messages

WhatsApp is a social media platform where participants exchange ideas. Many messages are posted and re-posted to friends or forwarded to other group platforms such that by the time a message gets to one, its source may not be traceable. Criminals have keyed into this area too by posting fake vacancies on the WhatsApp forum to attract job-seekers to their den. The following is a warning against such vacancies.

5. BEWARE! DON'T ATTEND ANY INTERVIEWS AT THIS ADDRESS.

Olabisi Close, MENDE, Maryland (Lagos Resident only) hr
080-7464-5567
Please beware of this Address
They are Kidnappers and ritualists...
Kindly spread it. We never know who we might save. Sent as received.

This text rests on the shared knowledge among Nigerians about the existence of ritualists. Ritualists in Nigeria are dangerous people to whom kidnappers sell kidnap victims. Ritualists are said to use human beings or human parts for rituals or charms. So, people visit ritualists to make money rituals or charms that will enable them to win elections into their desired public offices, make them extremely rich or get something extraordinary. Given the text above, readers, especially job-seekers, are warned not to visit a particular address in Lagos to avoid falling victim of ritual killing. Perhaps, this is a rider to the account of a woman who went for an interview in a secluded place. She escaped through a tip-off from a member of her church who happened to be a gateman in the house. The issue here is that fraudsters exploit all situations, including joblessness to make money at all costs. They remain faceless and difficult to apprehend because of the anonymity provided by the internet.

Sometimes, some seemingly innocuous messages on WhatsApp turn out to be links to gambling websites. For instance, the following messages were posted on WhatsApp, but the links lead to gambling sites:

6. OMG! Have you seen this? xxxv.xxuxi.com³
7. See this now xxx.xxvxa.com

The messages look harmless and seem to lead to a great opportunity that someone may want to see. However, they actually lead to gambling websites. This is a means of luring unsuspecting youths into gambling.

On Nairaland, there are regular invitations to members to meet 'sugar daddies' or 'sugar mummies'⁴ with promises of money. Interested persons' phone numbers are normally requested. Since it is now widespread, it is no longer strange to have requests for sugar mummies on Nairaland. However, it is believed that such sugar daddies and mummies use charms to 'steal the destined fortunes' of people who make love to them or that they make love to.

Cyber-Attack Through Facebook

Facebook is a bigger forum than the WhatsApp. The first observation of fraudsters' antics is that they would send a friend's request. A careful user of Facebook would look at the profile of the would-be friend. For normal person's Facebook account, the profile will be populated with different stories or activities. For fraudsters, they have very scanty information on their profile pages. In some cases, faces of white people are used as display pictures. One thing is certain here: the photos were stolen from some online web pages and reused. This is identity theft. In addition, they try to legitimise their identity by seeking friendship with normal innocent people. Once that is achieved, they start their nefarious activities. One way is to try and seduce the target.

A poster on the Nairaland received such an invitation and accepted the friend request of a supposedly white lady, who claimed to be chatting from London. In the course of their conversation, she requested webcam chat, but the poster said his laptop had problems with video call. She requested his phone number and home address, and he supplied them. The lady then told him that she had sent him a package containing a laptop through a company called RM Logistics Courier Service. She claimed to have paid for the export tax and transport, but that the company policy denied her payment for the clearing, and that the receiver was to pay for that. In lieu of that, she claimed to have hidden £400 inside the keyboard of the laptop. She advised the recipient to clear it since the company does home delivery. She sent a picture of a beautiful golden Apple laptop. Thereafter, she wrote that she placed an iPhone inside for him as a surprise. She advised him to expect the company's call on Thursday.

For a poor, unemployed or greedy person, this may be seen as a gift from a benevolent person. However, a reasoning fellow would wonder what benefit the white lady would derive by giving out such gifts to a total stranger. The second issue is that she claimed to have hidden 400 pounds in the laptop. Apart from its illegality, when the money is converted to the local currency, it amounts to about ₦185,000.00, an amount sufficient to buy another laptop in Nigeria! This is an appeal to the greed of the recipient. A greedy person may not think of clearing alone, he might think of the huge sum and what he could do with it after clearing the laptop. Finally, perhaps as an afterthought, she claims to have included an iPhone, a very expensive phone, as a surprise. Since she has already said so, is it still a surprise? The real intention is to appeal to the target's greed and brainwash him to desire the package very much. And the company whose name is fake cannot be located. If there is need to invite the police or go to court, there is no name or address attached to the company.

The poster narrated this experience on the Nairaland Forum for advice because he suspected it was a scam⁵. Members confirmed his fears. They said it is a regular means of scamming people. One member said her friend lost ₦40,000 in a similar scam. The recipient will be milked of any amount of money criminals can get from him and he will not get any parcel eventually. One person also noted that the white lady's use of English did not look like that of someone in London; it was a Nigerian variety of English.

Another poster brought a related matter to the Nairaland forum⁶ he was duped to the tune of ₦12,000 by a Facebook friend who promised to get him a job. He was asked to pay some money in advance. Still on Nairaland, scammers dupe people of their money through games. A dupe got a fake game he played in gambling and lost despite all assurances. When the dupe complained, he was promptly removed from the WhatsApp group chat⁷. In a related development, a man who paid to buy data online was also duped. He transferred the requested amount into the scammer's account but the scammer did not send the data paid for⁸.

Facebooks accounts are also hacked such that hackers assume ownership of the account. Such fraudsters send messages to contacts on the account claiming to be at one meeting or being stranded at a place where they cannot get recharge cards to buy. Such contacts are then requested to send recharge card numbers online for the fraudster to change to liquid cash thereafter. Some gullible people fall for this scam; some do not, requesting that the Facebook friend (assumed by the fraudster) send his or her phone number and that they would credit it directly or send the recharge card PIN into it. Some people also impersonate other people for nefarious activities. A man allegedly opened a social media account in Godson's name to defraud his unsuspecting fans. He lifted Godson's videos and photographs and used them to convince his targets and then proceeded to ask for their nude photographs⁹. This is a case of identity theft.

The Facebook is also used to lure people into places where they are violated or used for rituals. Many accounts exist where a male will request friendship from a female online. After she accepts, they will keep chatting and, in the process, arrange for a date. When the target shows up, they are usually molested by many males or decapitated for sale to ritualists. Gory tales of these appear on Facebook and in newspapers. Some that escaped such attacks exposed the modes of operation of such criminals. There was the case of a university student who became friends with a man she met on Instagram.¹⁰ When they met in a hotel, she was drugged and abused. The man took photographs of her state of nudity and recorded the sex sessions on video. These later became tools for blackmail. This is abuse. However, the man was later arrested by the police.

It is also becoming widespread that lovers will meet and have intimacy, but the male partner will record the acts and later use it for blackmail. Two ladies were drugged and violated when they visited a man one of them had met via Facebook. The man and his friend who was with him when the girls visited made a video of their love sessions and posted it on the WhatsApp and it later got posted on a porn site¹¹. In another case¹², a lady got very emotional with a man she had met only on Facebook. She sent different nude photos to him. The man turned around to request a video call with her posing nude, and threatened to post her nude pictures which he had on the Internet if she did not oblige him¹³. The only saving grace is that the police are catching up with the criminals, provided the victim is bold enough to report the case. Nevertheless, the acts constitute an abuse of the internet, a cybercrime.

A subtle part of it is that young females, usually claiming to be undergraduates, often request friendship from random males on Facebook. They easily agree to advances from the males. In the process, they request transport fare, purportedly to take them to the man's house for a date. Since the initial request is often little, say, as low as N3,000 for a long-distance trip, an unsuspecting man may pay the money into the bank account provided by the female. After payment, she may make further requests until the male gets frustrated and wakes up to the reality that he has been duped. Another aspect of it is that some female university undergraduates use this medium and method to engage in subtle prostitution, called 'runs'. Having made contacts on Facebook, they offer sex for money to random males, charging according to the ability of the client.

Online materials abuse is also capable of dehumanising the youth. A 27-year old Microbiology graduate and Nairaland user recounted how she accepted a friend request of an Indian man, exchanged nude pictures with him and also engaged in video chat with him.¹⁴ Now, she is addicted to it and masturbates any time she is alone, even when in church. She feels guilty, and cries out for help. This person used the cover of anonymity provided by the Nairaland forum to shout out. We may not know now how many other victims of this kind of abuse are suffering in silence.

Fraudsters can also play on the intelligence of humanitarian people. A scammer posted a photo of a very sick child, claiming it had congenital heart disease, and asking for ₦12.000 to balance the money he already had¹⁵. Beside the child's picture, the scammer posted what looked like a medical report on the child. Medical doctors on the site enlightened online readers that the medical report was fake; in fact, it was gibberish! The scammer had tried to hoodwink people with the squiggles on the paper since doctor's handwritten reports are usually illegible to lay people.

Finally, there is also the aspect of cyber bullying on Facebook. A private school owner had sought advice regarding how to solve a particular problem in the school she managed from members of her group on Facebook. Rather than give the advice she requested, commentators took her up on her incompetence in the use of the English language. She was thoroughly humiliated. Eventually, she wrote, bemoaning her fate and announcing her withdrawal from the group. That was the result of cyberbullying.

Advertising

For the purposes of celebrating birthdays, some may upload their nude or half nude pictures on the social media. They are quite oblivious of the harm they are causing the society, especially the youths. An example is the story of a girl dressed in bikini whose pictures appear in *National Helm*, an online newspaper¹⁶. Any youth that comes across the photo may want to emulate her. However, this is cultural degradation. Traditionally, the underwear is supposed to be worn underneath the clothes. Now, this culture has been debased to the extent that its abuse is now displayed on the social media. The question is: what do ladies gain through this act? It is simply to let the pictures go viral, such that many social media commentators will *like* it. The more *likes* it attracts, the more satisfied, fulfilled or highly rated the profile owner is assumed to be.

According to a Nairaland thread¹⁷, a lady may start posting on her profile page with decent pictures and stories, and get, say 3 *likes* and 0 comments. Dissatisfied and frustrated, she may post a sexy picture (possibly wearing a skimpy dress in the picture) and get 50 likes and 20 comments. Encouraged by the results, she may take a picture at the pool where she's dressed in only bikini, and the result may go up to 450 *likes* and 100 comments. This encourages her to post more revealing photos and write more morally depraving stories on her page. She becomes insatiable and continues to post more revealing pictures of herself just to get the attention she desperately desires. The cybercrime world has thus successfully won another convert!

Perhaps, the most brazen acts came from a woman who posted a video of herself engaged in acts of lesbianism; and a student who uploaded her nude pictures and masturbation video.¹⁸ Another lady has also put her nude and erotic pictures for sale at ₦8,000/\$25 each and masturbation videos for \$40 each¹⁹. This confirms the claim that sex sells, but at whose expense?

Perhaps, more worrisome is the fact that some people traffic in women using the social media as advert platform²⁰. Beautiful ladies in different stages of nudity (from partial to total) are displayed on the internet for interested men. The men get across to the organisers and make their choices. The ladies travel to any place their 'services' are required at a fee. Although it is based in South Africa, it targets Nigerian clients. According to the www.ladiesgist.com blog, the organisation used the name Feline Management and Innovative Models as a smokescreen to shroud its activities. Curiously, some of the girls may not know they are being pimped; they get to know when they experience carnal abuse by clients. At the extreme, they may disappear without any trace or be found dead. A commentator to the blog said she was molested continuously by 6 men and given R20,000, and the organisers paid her 'to keep quiet'. She took the money and said nothing because she was too ashamed. Just like Feline Management and

Innovative Models, Social Exchange Market is alleged to be pretending to be a charity organisation.²¹ The organisation is said to be scam like the defunct Mavrodi's Ponzi scheme where members were encouraged to pay in some money to receive multiples of their investment in a short time.

Another incident was a job scam²². The victim applied for a job advert placed on Nairaland and was interviewed on phone. He was asked to do a medical test of fitness and given an account to pay the test fees into. Once he paid the amount, he realized he had been duped: there were no tests and no job!

Cloning of Financial Instruments

Many atrocities are carried out at different ATM spots. One of them is cloning. Users of the machine may just insert their cards into it to withdraw money oblivious of the fact that some fraudsters had programmed the machine to store their card's PIN numbers. After the users leave, the fraudsters will come back to retrieve the number, make a duplicate copy of the cards and use them to withdraw all the money in the accounts. Hence, users are advised to cancel previous transactions before inserting their cards. Cancelling previous transactions is expected to wipe off any pre-programmed cloning device that could have been installed on the ATM.

Cloning is not limited to ATMs. Some people had bought things and paid by using their ATMs on POS presented to them at shops and supermarkets. Some of such cards had also been cloned and the victim's money stolen. A vigilant vehicle owner prevented this from happening to him when he caught petrol station attendants trying to duplicate his card number. The need for vigilance in this kind of transaction cannot be overemphasised.

SOLUTIONS AND RECOMMENDATION

The first piece of advice is that one should not disclose any personal information or send one's photos to strangers online as they may be misused. Jack et al. (2016: 46) observe that victims "are usually the gullible, greedy and inexperienced and those desperate for quick money or love and relationships". They advise that individuals should observe safety rules by not revealing personal information and banking details to strangers.

One should also watch whatever one's children are doing on the Internet and use content filtering software on their computers (Jack et al. 2016). This will enable parental guidance and advice. Kamini also advised that people install latest antivirus and update them regularly to guard against attacks; and back up data in order to avoid loss in case of virus contamination. Web site owners are advised to install a security programme that gives control over cookies and sends information back to the site; and put host-based intrusion detection devices on servers.

In addition, the public needs to be educated on the existence and negative effects of cybercrime. Hence, jingles should be aired on radio and television to educate the public on how to identify cybercrimes and subsequently avoid being duped. This will not only protect the innocent people, it will also discourage fraudsters engaged in the crime. They should also be taught on how to avoid playing into the hands of fraudsters. Such acts include protecting their systems from cyber attacks, avoiding suspicious offers and protecting their financial and other relevant information from the public glare.

Individuals should also control their greed as well as love for money and the opposite sex. They should also not jump at seemingly good offers, especially from total strangers. More importantly, they should study online documents carefully for grammatical correctness and reasonable propositions, as these may give clues to identifying fake proposals.

It has also been suggested that every Nigerian should report cybercriminals regardless of their social affinity. Corporate bodies are advised to pool resources together to fight cybercrime, a common enemy, and protect their Internet resources and safeguard their operations through appropriate mechanism. They should sponsor bills against cybercrimes to enhance their business. The government is also advised to make more stringent laws and prescribe punishments to offenders (Idoko & Ugwuanyi, 2015). One of these is forfeiture of the proceeds of the crime to the government.

Government should further strengthen the Cybercrime Act of 2015 to ban wanton display of raunchy materials capable of destroying the youths of the nation. Although there is a section on ban of child pornography, a clever lawyer may claim that photographs in bikini do not constitute child pornography. Hence, the law needs to be strengthened as new cases of cybercrime or abuse come to the fore. Government should also provide adequate training to law enforcement, intelligence and security agencies on how to track down offenders (Okeshola & Adeta, 2013)

Finally, Boniface & Michael (2014) propose a design to monitor internet users' activities in order to curb cybercrime. This involves redefining the operations of Internet Service Providers (ISPs) which requires authentication of users before they access the Internet. This is expected to ease monitoring and apprehension of Internet offenders.

FUTURE RESEARCH DIRECTIONS

This study has discussed some aspects of cybercrime perpetrated on some social media platforms largely as reported on Nairaland. It would be necessary to conduct research on individual members of the platforms to provide first-hand experiences of cybercrimes they have had. Perhaps, we will get to know the ramifications of the problem and the government will be better advised on how to stem the tide. It may also be necessary to study other online platforms such as Eskimi, 2go, Twitter and Instagram in detail. A proper scrutiny of participants may yield great revelations about cybercrime in these places.

CONCLUSION

From the foregoing, we can make some inferences. The first thing is that cybercriminals assume a particular identity plausible enough to the target victim. Fraudsters get close to the target victims, sometimes use terms of endearment and generally make themselves acceptable to the would-be victims before they start the process of attacking them. They may exploit different situations such as unemployment, greed, stupidity, poverty or promiscuity to get close to the target. Once they get the target's weak point, they latch on to it and execute their plans.

Again, some targets become pawns in the hands of fraudsters because they are also dishonest, gullible, impatient, careless or carefree. Some people like the allure of the world, while some want to show their elevated status by assuming absolute knowledge of goings-on on the internet. In so doing, they hide information from friends and colleagues who could advise them. Yet, some are also selfish as well as greedy, such that they fall easy prey to the whims of the cybercriminal.

Some internet users are not computer savvy, but to acquire their practical computer knowledge, they go online and fall into traps. Some did not want to watch pornography, but they stumbled on it and got hooked; some wanted to show off their beauty, they ended up overdoing it and getting into wrong hands. Yet, some want to become a celebrity overnight; they attract dangerous elements to themselves by what they post. More worrisome is that many youths have sophisticated phones and because they are free from the public glare and from parental and other controls, they launch themselves into the Internet, unaware of the many cybercriminals prowling the web space. They all make themselves easy target for criminals.

Finally, many parents have relaxed their vigilance on their children or wards. They are negligent in their parental duty and their children, in the name of civilization, do anything they desire. It seems that a level of observation of the traditional/cultural norms which preach decency and modesty in what one does could save some children if they adhere to the culture.

These are weaknesses that the cyber-criminal exploits to attack individuals and the society. Each Nigerian ICT user should be careful and use the internet intelligently. Users need to guide against such attitudes to be free from cyber-attacks.

REFERENCES

- Aribake, F. O. (2015). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A conceptual Review. *International Journal of Trade, Economics and Finance*, 6(5), 272–277. doi:10.18178/ijtef.2015.6.5.481
- Ayofe, A. N., & Osunade, O. (2009). Towards Ameliorating Cybercrime and Cybersecurity. *International Journal of Computer Science and Information Security*, 3(1), 1–11.
- Boniface, K. A., & Michael, K. A. (2014). Curbing Cybercrime by Application of Internet Users' Identification System (IUIS) in Nigeria, *World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering*, 8(9), 1582–1585.
- Chawki, M. (2009). Nigeria Tackles Advance Free Fraud. *Journal of Information, Law & Technology*, 1, 1-20. Retrieved from http://go.warwick.ac.uk/jilt/2009_1/chawki
- Dagaci, Magaji, & Damagun. (2014). Cybercrimes and Victimization: An Analysis of Economic Cost Implications to Nigeria. In *Handbook on the Emerging Trends in Scientific Research*. ICETSR.
- Idoko, N. A., & Ugwuanyi, R. N. C. (2015). *Cyber Crimes: Bane of Nigeria's Information Growth and Utilization*. Retrieved from www.jaistonline.org
- Jack, J. T. C. B., & Ene, R. W. (2016). Cybercrime and the Challenges of Socio-economic Development in Nigeria. *JORIND*, 14(2), 42–49.
- Kamini, D. (2011). Cyber Crime in the Society. *Problems and Preventions Journal of Alternative Perspectives in the Social Sciences*, 3(1), 240–259.
- Maitanmi, O., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Cyber Crimes and Cyber Laws in Nigeria. *International Journal of Engineering Science*, 2(4), 19–25.
- Nwogwugwu, U. C., & Uzoechina, B. I. (2015). Impact of Economic Crimes on Nigeria's Economic Prosperity under A Democratic Framework. *International Journal of Business and Management*, 10(9), 163–184. doi:10.5539/ijbm.v10n9p16

Ojeka, S. A., Ben-Caleb, E., & Ekpe, E.-O. I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing*, 7(2), 340–346.

Okeshola, F. B., & Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), 98–114.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention *FUOYE. Journal of Engineering Technology*, 1(1), 37–42.

Symantec. (2016). *Cyber Crime and Cyber Security Trends in Africa*. Retrieved from www.symantec.co/theme/cyber-security-trends-africa

Toyo, D. O. (2017). ICT Use and Its Impact in Combating Cybercrimes in Abraka, Delta State. *Nigeria Research Journal of Mass Communication and Information Technology*, 3(1), 10–23.

KEY TERMS AND DEFINITIONS

Cashless Policy: A policy that discourages the use of huge raw cash for transactions but encourages the use of bank transfer, ATM card, POS, and other financial instruments for transferring cash in transactions.

Cloning: Creating a replica of websites or cards with intent to defraud.

Cyberattack: Any form of injury done to a network or individual through the internet (e.g., cyber stalking, cyber bullying, and malware).

Cybercrime: Any crime committed using the ICT platform. These may be child pornography, phishing, cyber terrorism, etc.

ICT: Information communication technology; involving the use of computer, phones, and the internet in managing information.

Identity Theft: Assuming the identity of another individual by using their photographs, profiles, or e-mail accounts to act in their capacity for nefarious activities.

Netrespass: Infiltrating another internet user's space and carrying out unauthorised activities (e.g., trespass).

Victim: The individual or entity that suffers the effect of cyberattacks.

ENDNOTES

¹ UNILAG lecturer in sex scandal as student releases his nude photos. <https://www.pulse.ng/communities/student/unilag-lecturer-in-sex-scandal-as-student-releases-nude-photos-id444278.html>

² Alleged Sex Scandal: UNILAG releases panel's interim report. <https://www.premiumtimesng.com/news/more-news/276692-alleged-sex-scandal-unilag-releases-panels-interim-report.html>

³ Source: WhatsApp message on a chat platform.

⁴ a polite reference to male of female sex partners with financial or other benefits.

⁵ Please Guys Confirm with me If this Is a Scam. www.nairaland.com

⁶ This Lady Presly Chiamaka on Facebook Scammed me of 12k. www.nairaland.com

⁷ Be careful of Latest Scam in Town. www.nairaland.com

- 8 Fraud Alert. www.nairaland.com
- 9 Man Arrested for Impersonating Mike Godson and Collecting Nudes from His Fans. www.nairaland.com
- 10 How Instagram Friend Drugged, Sexually Assaulted Unilorin Student. www.Nairaland.com
- 11 Guys Drug and Rape 2 Girls They Met Via Facebook in Lagos. www.Nairaland.com
- 12 Man Records Lover During Sex, Uses it to Extort Money From Her. www.nairaland.com
- 13 Onitsha Man Threatens to Leak Nude Photos of Facebook Girlfriend Online. www.nairaland.com
- 14 Can God Forgive me of my Secret Sin of Masturbation. www.nairaland.com
- 15 Fraudster Exposed by Twitter Users After He Shared Photo of a Sick Child. www.nairaland.com
- 16 Lady Poses with Her Friends in Pant and Bra as She Celebrates Birthday. www.nationalhelm.com
- 17 How Slay Queen Use to Start. www.nairaland.com
- 18 1. Cucumber Chidinma Hits Internet Again, Shows Off Her Hot Curves. www.Nairaland.com
2. 100 Level Student Caught With Stolen Phones, Charms Dripping With Blood. www.Nairaland.com
- 19 Nigerian Lady Puts Her Nude Pics for Sale at #8,000 Each. www.naraland.com.
- 20 Shocking Details of South African Sex Trafficking Ring Nigerian Governors and Rich Men Patronise. www.ladiesgist.com.
- 21 Shocking Revelation: Social Exchange Market Busted as Fraudulent Programme. <https://huntersinternational.org>
- 22 Fraudsters on Nairaland. www.nairaland.com

Machine Learning and Cyber Security: Future Potential of the Research

Vardan Mkrttchian

 <https://orcid.org/0000-0003-4871-5956>

HHH University, Australia

Sergey Kanarev

Penza State University, Russia

Leyla Gamidullaeva

 <https://orcid.org/0000-0003-3042-7550>

Penza State University, Russia

INTRODUCTION

Cyber security has become an important subject of national, international, economic, and social importance that affects multiple nations (Walker, 2012). Many countries have come to understanding that this is an issue and has developed policies to handle this in an effort to mitigate the threats (Dawson, Omar, & Abramson, 2015). To address the issue of cyber security, various frameworks and models have been developed. Traditional approaches to managing security breaches is proving to be less effective as the growth of security breaches are growing in volume, variation and velocity (Bhatti & Sami, 2015). The purpose of this article is to show what future cyber security as engineering science and technology expects. In addition, the authors propose future solutions for the use of computer with a Sleptsov Net-processor when it will be actually created and practically implemented. The authors of the article did not consider the credibility issues of Sleptsov network computing but completely trusted the creator of Sleptsov net as a processor, based on open sources, in particular on publications and webinars of IGI Global (Zaitsev, 2016; Zaitsev, et al., 2016; Zaitsev, 2018). Based solely on these publications the authors research the emerging trends and perspectives of digital transformation of the economy using machine learning with avatar-based management at the platform of Sleptsov Net-processor and propose further prospects for development of hyper-computation (Mkrttchian, et al., 2019).

BACKGROUND

Many researchers compare machine learning solutions for cyber security by considering one specific application (e.g., Buczak and Guven, 2016; Blanzieri and Bryl, 2008; Gardiner and Nagaraja, 2016) and are typically oriented to Artificial Intelligence experts.

DOI: 10.4018/978-1-5225-9715-5.ch070

The term “cyber security” refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware devices and software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The associated field of professional endeavor, including research and analysis, aimed at implementing those activities and improving their quality (Jenab, et al., 2018).

At the same time, our previous research of the problem of cyber security showed that cyber security is a section of information security, within the framework of which the processes of formation, functioning and evolution of cyber objects are studied. It is necessary to identify sources of cyber-danger formed while determining their characteristics, as well as their classification and formation of regulatory documents, implementation of security systems in future. However, working on the application of the machine learning for Cyber Security applications with the use of developed by the authors Avatars-Based Management techniques, we came to the conclusion that this is not so, and the built-in cyber security systems can be destroyed by the same artificial intelligence.

The search for a solution to this discrepancy leads to a thought about advantages of natural intelligence displayed by humans where everything is interconnected, logical and protected (Mkrttchian, et al., 2015).

This paper is specifically aims to research the emerging trends and perspectives of cyber security development in the conditions of digital economic transformation using machine learning with avatar-based management at the platform of Sleptsov Net-processor, and to identify their main limitations.

Sleptsov net concept mends the flaw of Petri nets, consisting in incremental character of computations, which makes Sleptsov net computing a prospective approach for ultra-performance concurrent computing (Zaitsev, 2018).

A Sleptsov net (SN) is a bipartite directed multi-graph supplied with a dynamic process (Zaitsev, 2016). An SN is denoted as $N=(P,T,W,\mu_0)$, where P and T are disjoint sets of vertices called places and transitions respectively, the mapping F specifies arcs between vertices, and μ_0 represents the initial state (marking). The mapping $W: (P \times T) \rightarrow N \cup \{-1\}$, $(T \times P) \rightarrow N$ defines arcs, their types and multiplicities, where a zero value corresponds to the arc absence, a positive value – to the regular arc with indicated multiplicity, and a minus unit – to the inhibitor arc which checks a place on zero marking. N denotes the set of natural numbers. To avoid nested indices we denote $w_{ij} = w(p, t)$ and $+ =$. The mapping $\mu: P \rightarrow N$ specifies the place marking (Zaitsev, 2018).

Based on the previous research, performed by D. Zaitsev (2018; 2019), the main conclusion was drawn that Sleptsov networks are executed exponentially faster than Petri nets that makes it possible to recommend them as a parallel computing model for subsequent practical implementation.

Calculations on the networks of Sleptsov acquire all new applications presented in the works. First of all, computations on Sleptsov networks may be used for those applications in which parallel programming style can bring significant acceleration of computations.

Effective practical implementation of computations on Sleptsov networks requires the development of appropriate specialized automation systems for programming and hardware implementation of processors of Sleptsov networks. In addition, further development of theoretical methods of proving the correctness of programs in the language of Sleptsov networks and the development of universal networks that use mass parallelism are needed.

The advantages of computing on the Sleptsov networks are visual graphic language, the preservation of the natural domain parallelism, fine granulation of parallel computing, formal verification methods for parallel programs, fast mass-parallel architectures that implement the computation model (Zaitsev, 2018).

FOCUS OF THE ARTICLE

Machine learning (ML) was introduced in the late 1950's as a technique for artificial intelligence (AI) (Ambika, 2018). Over time, its focus evolved and shifted more to algorithms that are computationally viable and robust. One of the classical definitions of Machine Learning is the development of computer models for learning processes that provide solutions to the problem of knowledge acquisition and enhance the performance of developed systems (Duffy, 1995).

Machine learning is the use of artificial intelligence (AI) that provides systems with the capability to learn and automatically improve from experience (data) without being explicitly programmed. Machine learning focuses on developing computer programs that can access data and use them to learn by themselves.

Ideology of Machine Learning based on the principles of multiple use (reusability) and free distribution (share ability) copyright courses. Therefore, developers of training courses must adhere to generally accepted standards. To date, the most widely used models of the following courses:

1. Model IEEE LOM (Learning Object Model), developed by the LTSC (Learning Technology Standard Committee) in 2002. The entire set of learning objects is divided into 9 composite hierarchies (categories): General (General), life cycle (Life Cycle), metadata (Metadata), technical (Technical), education (Education), legal (Rights), communication (Relation), annotation and classification (Annotation and Classification).
2. System specifications consortium IMS (such as egg Content Packaging Specification, Metadata Specification, Digital Repositories Interoperability, Digital Repositories).
3. Specifications Committee AICC (Aviation Industry Computer-Based Training Committee) originally intended for the development of computer-based training systems and technologies in the aviation industry.
4. Specification SCORM (Shareable Course Object Reference Model), developed in the framework of the ADL (Advanced Distributed Learning), carried out by the Ministry of Defense. This is the industry standard for exchange of training materials based on tailored specifications ADL, IEEE, IMS. AICC. SCORM is the basis of the model modular design of educational material by separating the individual autonomous educational units (SCO - Shareable Content Objects) and their representation in the Web- specific repositories. SCO modules can be assembled together in various combinations and compiled into electronic textbooks using LMS- system. Thus, if in the first E-Learning systems, a teacher was expected to collect their own training courses to keep in his personal computer, and then manually organize a nationwide educational content, with the advent of such specifications as SCORM, this work is automated with the possibility of using Web 2.0 technologies and service-oriented approach (Mkrttchian, et al., 2019).

Another pressing problem of modern machine learning systems is the problem of creating a student model based on the tracking of personal information related to learning trajectories passing on various training modules or web-services, the courses tendered tests. For these purposes, there is also a range of specifications, the most famous of which are:

- IEEE PAPI (Personal and Private Information);
- IMS LIP (Learner Information Package).

It uses the language XML (eXtension Markup Language) to write to the user's profile his curriculum vitae, teaching history, language skills, preferences to use computer platforms, passwords, access to training, etc. These data are then used to account for the individual characteristics of the student in determining the best means and methods of teaching.

Competency assessments for learning are also used standardized specifications, which were developed and presented in the recent authors' work (Mkrtychian, et al., 2019). In this work, the authors consider different issues related to the modeling supercomputer with Sleptsov Net-processor to visualize of a report on the work of Cyber Security system.

Having considerable experience in Intellectual Control and Communication, Avatar-Based Learning, Teaching and Training, and Avatar-Based Management, there is a need in modelling a joint system of Machine Learning with Avatar-Based Management with the use of Sleptsov Net-processor.

We define as an Avatar-Based Management (A-BM) model variability hypergraph VMG, consisting of two sets and predicate:

$$VMG = (V, U, P), \quad (1)$$

Set V describes the structure of a hypergraph on the vertex level:

$$V = \{v_{i,(weight)}\}, i = 1, 2, \dots, N, \quad (2)$$

where N – is the total number of peaks is corresponding to the total number of characteristics of the A-BM model variability; weight - vertex weight in form n.1.1.1 corresponding to the index of the corresponding characteristics in the hierarchical structure of the A-BM model variability.

Set U has a capacity corresponding to the number of possible configurations of the A-BM:

$$U = \{u_j\} ; j = 1, 2, \dots, K, \quad (3)$$

where K - the numbers of hyperedges.

Obviously, depending on the size and structure of each elements of Block diagram the Model of Platform of the supercomputer with Sleptsov Net-processor in the Support Cyber Security Applications (fig.2), from the technical and communications capabilities available to the user at some point and some other features of the cardinality of the set U can vary significantly.

Predicates P - determines incidence of vertices and hyperedges of each layer. P is defined on the set of all pairs $(v \in V, u \in U)$. Truth domain predicate P is the set R of variable cardinality $Bt \neq \text{const}$:

$$F(P) = \{(v, u) \mid P(v, u)_r\}, \quad (4)$$

Where $v \in V, u \in U, r \in R = \{1, 2 \dots B_r\}$

Variability of the cardinality of R is due to the same causes as the variability of U in Equation 3.

Considered a set-theoretic representation of the A-BM model to determine the variability of the matrix representation of this A-BM model is useful for creating software for Machine learning application with Avatar-Based Management technique use. Matrix representation (incidence matrix size $N \times K$) hypergraph will have the form (Mkrttchian, et al., 2014) (5):

$$M_f = || m_{ij} ||_{N \times K}, \quad (5)$$

Where:

$$1, \text{ if } (v_i, u_j) \in F(P), v \in V, u \in U$$

$$m_{ij} = 0, \text{ if } (v_i, u_j) \notin F(P), v \in V, u \in U$$

In some cases it is more convenient to use the matrix of connected vertices of the hypergraph (Equation 6), which has a size $N \times N$ and reflects pairwise connectivity relations through vertices incident hyperedges).

$$M_c = || m_{ij} ||_{N \times N}, \quad (6)$$

where:

$$1, \text{ if } (v_i, v_j) \exists u_k, (v_i, u_k) \in F(P), (v_j, u_k) \in F(P), v \in V, u \in U$$

$$m_{ij} = 0, \text{ if } (v_i, v_j) \neg (\exists u_k), (v_i, u_k) \in F(P), (v_j, u_k) \in F(P), v \in V, u \in U$$

The authors developed a Block diagram of the model of platform for supercomputer with Sleptsov Net-processor in support cyber security applications (Mkrttchian, et al., 2019), which allows to implement the hypergraph, in which weights of vertices correspond to indices characteristics in the A-BM model supercomputer with Sleptsov Net-processor model and the hyper-cores correspond possible A-BM model configurations.

CONCLUSION

In this article, the authors studied machine-learning application with the use of Avatar-Based Management technique for cyber security issues. Our previous research devoted to the cyber security problem showed that cyber security is a section of information security, within the framework of which the processes of formation, functioning and evolution of cyber objects are studied. It is necessary to identify sources of cyber-danger formed while determining their characteristics, as well as their classification and formation of regulatory documents, implementation of security systems in future. However, working on the application of the machine learning for Cyber Security applications with the use of developed by the authors Avatars-Based Management techniques, we came to the conclusion that this is not so, and the built-in cyber security systems can be destroyed by the same artificial intelligence (Mkrttchian, et al., 2019).

The author concluded that machine learning with Avatar-Based Management at the platform of the Sleptsov Net-processor is the future solutions to hyper-computations in the support cyber security applications.

ACKNOWLEDGMENT

The reported study was funded by RFBR according to the research project No. 18-010-00204_a.

REFERENCES

- Ambika, P. (2018). Machine Learning. In P. Raj & A. Raman (Eds.), *Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science* (pp. 209–230). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-5972-6.ch011
- Bhatti, B. M., & Sami, N. (2015). Building adaptive defense against cybercrimes using real-time data mining. *2015 First International Conference on Anti-Cybercrime (ICACC)*. 10.1109/Anti-Cyber-crime.2015.7351949
- Blanzieri, E., & Bryl, A. (2008). A survey of learning-based techniques of email spam filtering. *Artificial Intelligence Review*, 29(1), 63–92. doi:10.1007/10462-009-9109-6
- Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys and Tutorials*, 18(2), 1153–1176. doi:10.1109/COMST.2015.2494502
- Dawson, M., Omar, M., & Abramson, J. (n.d.). Understanding the Methods behind Cyber Terrorism. *Encyclopedia of Information Science and Technology, Third Edition*, 1539–1549. doi:10.4018/978-1-4666-5888-2.ch147
- Duffy, J. (1975). IFToMM symposium—Dublin, September 1974. *Mechanism and Machine Theory*, 10(2-3), 269. doi:10.1016/0094-114X(75)90030-0
- Gardiner, J., & Nagaraja, S. (2016). On the Security of Machine Learning in Malware C&C Detection. *ACM Computing Surveys*, 49(3), 1–39. doi:10.1145/3003816
- Jenab, K., Khoury, S., & LaFevor, K. (2016). Flow-Graph and Markovian Methods for Cyber Security Analysis. *International Journal of Enterprise Information Systems*, 12(1), 59–84. doi:10.4018/IJEIS.2016010104
- Jenab, K., Khoury, S., & LaFevor, K. (2018). Flow-Graph and Markovian Methods for Cyber Security Analysis. In I. Management Association (Ed.), *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 674–702). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-5634-3.ch036
- Mkrttchian, V. (2015). Use Online Multi-Cloud Platform Lab with Intellectual Agents: Avatars for Study of Knowledge Visualization & Probability Theory in Bioinformatics. *International Journal of Knowledge Discovery in Bioinformatics*, 5(1), 11–23. Doi:10.4018/IJKDB.2015010102

Mkrttchian, V., & Aleshina, E. (2017). *Sliding Mode in Intellectual Control and Communication: Emerging Research and Opportunities*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2292-8

Mkrttchian, V., & Belyanina, L. (Eds.). (2018). *Handbook of Research on Students' Research Competence in Modern Educational Contexts*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3485-3

Mkrttchian, V., Bershadsky, A., Bozhday, A., & Fionova, L. (2015). Model in SM of DEE Based on Service-Oriented Interactions at Dynamic Software Product Lines. In G. Kurubacak & T. Yuzer (Eds.), *Identification, Evaluation, and Perceptions of Distance Education Experts* (pp. 231–248). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8119-4.ch014

Mkrttchian, V., Bershadsky, A., Bozhday, A., Kataev, M., & Kataev, S. (Eds.). (2016). *Handbook of Research on Estimation and Control Techniques in E-Learning systems*. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-9489-7

Mkrttchian, V., Gamidullaeva, L. A., & Kanarev, S. (2019). Machine Learning With Avatar-Based Management of Sleptsov Net-Processor Platform to Improve Cyber Security. In M. Khan (Ed.), *Machine Learning and Cognitive Science Applications in Cyber Security* (pp. 139–153). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-8100-0.ch006

Mkrttchian, V., Kataev, M., Shih, T., Kumar, M., & Fedotova, A. (2014). Avatars “HHH” Technology Education Cloud Platform on Sliding Mode Based Plug- Ontology as a Gateway to Improvement of Feedback Control Online Society. *International Journal of Information Communication Technologies and Human Development*, 6(3), 13-31. Doi:10.4018/ijicthd.2014070102

Mkrttchian, V., Veretekhina, S., Gavrilova, O., Ioffe, A., Markosyan, S., & Chernyshenko, S. V. (2019). The Cross-Cultural Analysis of Australia and Russia: Cultures, Small Businesses, and Crossing the Barriers. In U. Benna (Ed.), *Industrial and Urban Growth Policies at the Sub-National, National, and Global Levels* (pp. 229–249). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7625-9.ch012

Walker, S. (2012). Economics and the cyber challenge. *Information Security Technical Report*, 17(1-2), 9–18. doi:10.1016/j.istr.2011.12.003

Zaitsev, D. (2018). Sleptsov Net Computing. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (4th ed.; pp. 7731-7743). Hershey, PA: IGI Global. Doi:10.4018/978-1-5225-2255-3.ch672

Zaitsev, D. A. (2018). Sleptsov Net Computing. In M. Khosrow-Pour, D.B.A. (Ed.), *Encyclopedia of Information Science and Technology*, Fourth Edition (pp. 7731-7743). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2255-3.ch672

Zaitsev, D. A. (2019). Sleptsov Net Computing. In M. Khosrow-Pour, D.B.A. (Ed.), *Advanced Methodologies and Technologies in Network Architecture, Mobile Computing, and Data Analytics* (pp. 1660-1674). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7598-6.ch122

ADDITIONAL READING

Bershadsky, A., Bozhday, A., Evseeva, J., Gudkov, A., & Mkrtchian, V. (2017). Techniques for Adaptive Graphics Applications Synthesis Based on Variability Modeling Technology and Graph Theory, In A. Kravets, M. Shcherbakov, M. Kultsova, & O. Shabalina, (Eds.), *Proceedings of CIT&DS 2017*, (pp. 169–179). Switzerland: Springer International Publishing AG. DOI: 10.1007/978-3-319-65551-2_33

Bershadsky, A., Evseeva, J., Bozhday, A., Gudkov, A., & Mkrtchian, V. (2015). Variability modeling in the automated system for authoring intelligent adaptive applications on the basis of three-dimensional graphics, In A. Kravets, M. Shcherbakov, M. Kultsova, & O. Shabalina, (Eds.), *Proceedings of CIT&DS 2015*, (pp. 149–159). Switzerland: Springer International Publishing AG. DOI: 10.1007/978-3-319-23766-4

Glотова, T., Deev, M., Krevskiy, I., Matukin, S., Mkrtchian, V., & Sheremeteva, E. (2015). Individualized learning trajectories using distance education technologies, In A. Kravets, M. Shcherbakov, M. Kultsova, & O. Shabalina, (Eds.), *Proceedings of CIT&DS 2015*, (pp. 778–793). Switzerland: Springer International Publishing AG. DOI: 10.1007/978-3-319-23766-4

Mkrtchian, V. (2011). Use ‘hhh’ technology in transformative models of online education. In G. Kurubacak & T. Vokan Yuzer (Eds.), *Handbook of research on transformative online education and liberation: Models for social equality* (pp. 340–351). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-60960-046-4.ch018

Mkrtchian, V. (2012). Avatar manager and student reflective conversations as the base for describing meta-communication model. In G. Kurubacak, T. Vokan Yuzer, & U. Demiray (Eds.), *Meta-communication for reflective online conversations: Models for distance education* (pp. 340–351). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-61350-071-2.ch005

Mkrtchian, V. (2015). Modeling using of Triple H-Avatar Technology in online Multi-Cloud Platform Lab. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3rd Ed.). (pp. 4162–4170). IRMA, Hershey: PA, USA: IGI Global. Doi:10.4018/978-1-4666-5888-2.ch409

Mkrtchian, V. (2016). The Control of Didactics of Online Training of Teachers in HHH University and Cooperation with the Ministry of Diaspora of Armenia. In V. Mkrtchian, A. Bershadsky, A. Bozhday, M. Kataev, & S. Kataev (Eds.), *Handbook of Research on Estimation and Control Techniques in E-learning systems* (pp. 311–322). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-4666-9489-7.ch021

Mkrtchian, V., Amirov, D., & Belyanina, L. (2017). Optimizing an Online Learning Course Using Automatic Curating in Sliding Mode. In N. Ostashevski, J. Howell, & M. Cleveland-Innes (Eds.), *Optimizing K-12 Education through Online and Blended Learning* (pp. 213–224). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-5225-0507-5.ch011

Mkrtchian, V., Aysmontas, B., Uddin, M., Andreev, A., & Vorovchenko, N. (2015). The Academic views from Moscow Universities of the Cyber U-Learning on the Future of Distance Education at Russia and Ukraine. In G. Eby & T. Vokan Yuzer (Eds.), *Identification, Evaluation, and Perceptions of Distance Education Experts* (pp. 32–45). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-4666-8119-4.ch003

Mkrtchian, V., & Belyanina, L. (2016). The Pedagogical and Engineering Features of E- and Blended Learning of Adults Using Triple H-Avatar in Russian Federation. In V. Mkrtchian, A. Bershadsky, A. Bozhday, M. Kataev, & S. Kataev (Eds.), *Handbook of Research on Estimation and Control Techniques in E-Learning Systems* (pp. 61–77). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-4666-9489-7.ch006

Mkrttchian, V., Kataev, M., Hwang, W., Bedi, S., & Fedotova, A. (2014). Using Plug-Avatars “hhh” Technology Education as Service-Oriented Virtual Learning Environment in Sliding Mode. In G. Eby & T. Vokan Yuzer (Eds.), *Emerging Priorities and Trends in Distance Education: Communication, Pedagogy, and Technology*. Hershey, PA, USA: IGI Global; doi:10.4018/978-1-4666-5162-3.ch004

Mkrttchian, V., Kataev, M., Hwang, W., Bedi, S., & Fedotova, A. (2016), Using Plug-Avatars “hhh” Technology Education as Service-Oriented Virtual Learning Environment in Sliding Mode. *Leadership and Personnel Management: Concepts, Methodologies, Tools, and Applications* (4 Volumes), (pp.890-902), IRMA, Hershey: PA, USA: IGI Global. Doi:10.4018/978-1-4666-9624-2.ch039

Mkrttchian, V., & Stephanova, G. (2013). Training of Avatar Moderator in Sliding Mode Control. In G. Eby & T. Vokan Yuzer (Eds.), *Project Management Approaches for Online Learning Design* (pp. 175–203). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-4666-2830-4.ch009

KEY TERMS AND DEFINITIONS

Hypercomputation or Super-Turing Computation: Is a multi-disciplinary research area with relevance across a wide variety of fields, including computer science, philosophy, physics, electronics, biology, and artificial intelligence; models of computation that can provide outputs that are not Turing computable.

Machine Learning: Is the use of artificial intelligence (AI) that provides systems with the capability to learn and automatically improve from experience (data) without being explicitly programmed.

Machine Learning Application With Avatar-Based Management Technique Use: Is a class of methods of natural intelligence, the characteristic feature of which is not a direct solution of the problem but training in the process of applying solutions to a set of similar problems.

Shareable Content Object Reference Model (SCORM): Is a collection of standards and specifications for web-based electronic educational technology (also called e-learning).

Sleptsov Net (SN): Is a bipartite directed multi-graph supplied with a dynamic process.

Perspective Tools to Improve Machine Learning Applications for Cyber Security

Vardan Mkrttchian

 <https://orcid.org/0000-0003-4871-5956>

HHH University, Australia

Leyla Gamidullaeva

 <https://orcid.org/0000-0003-3042-7550>

Penza State University, Russia

INTRODUCTION

Today security systems suffer from low detection rates and high false alarm rates. In order to overcome such challenging problems, there has been a great number of research conducted to apply Machine Learning (ML) algorithms (Tran, et al., 2012).

Machine learning techniques have been successfully applied to several real world problems in areas as diverse as image analysis, Semantic Web, bioinformatics, text processing, natural language processing, telecommunications, finance, medical diagnosis, and so forth (Gama, and Carvalho, 2012). Recent definition of machine learning is developed by I. Cadez, P. Smyth, H. Mannila, A. Salah, E. Alpaydin (Cadez, et al., 2001; Salah and Alpaydin, 2004).

The issues of the use of machine learning in cyber security are disclosed in many works (Anagnostopoulos, 2018; Edgar and Manz, 2017; Yavanoglu and Aydos, 2017; Khan, et al., 2014; Khan, 2019; Dinur, 2018). Using data mining and machine learning methods for cyber security intrusion detection is proposed by the authors (Kumar, et al., 2017). Object classification literature shows that computer software and hardware algorithms are increasingly showing signs of cognition and are necessarily evolving towards cognitive computing machines to meet the challenges of engineering problems (Khan, et al, 2014). For instance, in response to the continual mutating nature of cyber security threats, basic algorithms for intrusion detection are being forced to evolve and develop into autonomous and adaptive agents, in a manner that is emulative of human information processing mechanisms and processes (Khan, et al., 2014; Khan, 2019).

The maintenance of cyber security can significantly differ depending on the requirements for the control system, its purpose, the specificity of the managed object, the environmental conditions, the composition and state of the forces and controls, and the management order. Why do we need to distinguish between information and cyber security? What tasks can be achieved with this distinction?

This need is conditioned by the transition to a new socio-economic formation, called the information society. If earlier the problems of ensuring cyber security were relevant mainly for the military organization, in connection with the existence and development of the forces and means of information confrontation and electronic warfare, now such problems exist for the state as a whole.

Thus, the tasks of ensuring cyber security for today exist, both for the state as a whole, and for certain critical structures, systems and objects (Mkrttchian, et. al, 2019).

DOI: 10.4018/978-1-5225-9715-5.ch071

BACKGROUND

Modern economy networking now has become one of the most popular communication tools to have evolved over the past decade, making it a powerful new information sharing resource in world society. It is known, social-economy networking is the creation and maintenance of personal and business relationships especially through online social networking service that focuses on facilitating the building of social networks or social relations among people.

By embracing social networking tools and creating standards, policies, procedures, and security measures, educational organizations can ensure that these tools are beneficial.

The authors in this article show the essence, dignity, current state and development prospects of avatar-based management using blockchain technology for creation of new tools for machine learning applications (Mkrttchian, et al, 2016). The purpose of this article is not to review the existing published work on avatar-based models for policy advice, but to try an assessment of the merits and problems of avatar-based models as a solid basis for cyber security policy advice that is mainly based on the work and experience within the recently finished projects Triple H Avatar an Avatar-based Software Platform for HHH University, Sydney, Australia which was carried out 2008-2018 (Mkrttchian, et al., 2011,2012,2013,2014, 2015, 2016, 2017, 2018). The agenda of this project was to develop an avatar-based closed model with strong empirical grounding and micro-foundations that provides a uniform platform to address issues in different areas of digital economy. Particular emphasis was put on the possibility to generate an implementation of the model that allows for scaling of simulation runs to large numbers of avatars tools and to provide graphical user interfaces that allow researchers not familiar with the technical details of the implementation to design (parts of) the model as well as engineering and economy experiments and to analyze simulation output (Mkrttchian, 2015).

FOCUS OF THE ARTICLE

In this section, we discuss blockchain in relation to the visualization lifecycle including the following phases: identification, discovery, analysis, redesign, implementation, execution, monitoring, and adaptation. Using this lifecycle as a framework of reference allows us to discuss many incremental changes that blockchains might provide.

Process identification is concerned with the high-level description and evaluation of a company from a process-oriented perspective, thus connecting strategic alignment with process improvement. Currently, identification is mostly approached from an inward-looking perspective (*Dumas, et al., 2013*). Blockchain technology adds another relevant perspective for evaluating high-level processes in terms of the implied strengths, weaknesses, opportunities, and threats. For example, how can a company systematically identify the most suitable processes for blockchains or the most threatened ones? Research is needed into how this perspective can be integrated into the identification phase. Because blockchains have affinity with the support of inter-organizational processes, process identification may need to encompass not only the needs of one organization, but broader known and even unknown partners (Mkrttchian, et. al, 2019).

Process discovery refers to the collection of information about the current way a process operates and its representation as an as-is process model. Currently, methods for process discovery are largely based on interviews, walkthroughs and documentation analysis, complemented with auto-mated process discovery techniques over non-encrypted event logs generated by process-aware information systems (*Aalst, Wil, 2016*). Blockchain technology defines new challenges for process discovery techniques: the

information may be fragmented and encrypted; accounts and keys can change frequently; and payload data may be stored partly on-chain and partly off-chain.

For example, how can a company discover an overall process from blockchain transactions when these might not be logically related to a process identifier? This fragmentation might require a repeated alignment of information from all relevant parties operating on the blockchain. Work on matching could represent a promising starting point to solve this problem (*Cayoglu, 2014; Euzenat and Shvaiko, 2013 and other*). There is both the risk and opportunity of conducting process mining on blockchain data. An opportunity could involve establishing trust in how a process or a prospective business partner operates, while a risk is that other parties might be able to understand operational characteristics from blockchain transactions. There are also opportunities for reverse engineering business processes, among others, from smart contracts (Mkrttchian, et. al, 2019).

Process analysis refers to obtaining insights into issues relating to the way a business process currently operates. Currently, the analysis of processes mostly builds on data that is available inside of organizations or from perceptions shared by internal and external process stakeholders (Mendling, 2018). Records of processes executed on the blockchain yield valuable information that can help to assess the case load, durations, frequencies of paths, parties involved, and correlations between unencrypted data items. These pieces of information can be used to discover processes, detect deviations, and conduct root cause analysis (*Dumas, et al., 2013*), ranging from small groups of companies to an entire industry at large. The question is which effort is required to bring the available blockchain transaction data into a format that permits such analysis. Process redesign deals with the systematic improvement of a process. Currently, approaches like redesign heuristics build on the assumption that there are recurring patterns of how a process can be improved (*Mendling, 2018*). Blockchain technology offers novel ways of improving specific business processes or resolving specific problems. For instance, instead of involving a trustee to release a payment if an agreed condition is met, a buyer and a seller of a house might agree on a smart contract instead. The question is where blockchains can be applied for optimizing existing interactions and where new interaction patterns without a trusted central party can be established, potentially drawing on insights from related research on Web service interaction (Mkrttchian, et. al, 2019).

A promising direction for developing blockchain-appropriate abstractions and heuristics may come from data-aware workflows and diagrams. Both techniques combine two primary ingredients of blockchain, namely data and process, in a holistic manner that is well-suited for top-down design of cross-organizational processes. It might also be beneficial to formulate blockchain-specific redesign heuristics that could mimic how Incoterms define standardized interactions in international trade. Specific challenges for redesign include the joint engineering of blockchain processes between all parties involved, an ongoing problem for design (Mendling, 2018). Process implementation refers to the procedure of transforming a to-be model into software components executing the digital economy process. Currently, same processes are often implemented using process-aware information systems or business process management systems inside single organizations. In this context, the question is how the involved parties can make sure that the implementation that they deploy on the blockchain supports their process as desired. Some of the challenges regarding the transformation of a process model to blockchain artifacts are discussed by (*Mendling, 2018*).

It has to be noted that choreographies have not been adopted by industry to a large extent yet. Despite this, they are especially helpful in inter-organizational settings, where it is not possible to control and monitor a complete process in a centralized fashion because of organizational borders. To verify that contracts between choreography stakeholders have been fulfilled, a trust basis, which is not under control of a particular party, needs to be established. Blockchains may serve to establish this kind of

trust between stakeholders. An important engineering challenge on the implementation level is the identification and definition of abstractions for the design of blockchain-based business process execution. Libraries and operations for engines are required, accompanied by modeling primitives and language extensions of digital economy process. . Software patterns and anti-patterns will be of good help to engineers designing blockchain-based processes. There is also a need for new approaches for quality assurance, correctness, and verification, as well as for new corresponding correctness criteria. These can build on existing notions of compliance the more, dynamic partner binding and rebinding is a challenge that requires attention (Mkrttchian, et. al, 2019).

Process participants will have to find partners, either manually or automatically on dedicated market-places using dedicated look-up services. The property of inhabiting a certain role in a process might itself be a tradable asset. For example, a supplier might auction off the role of shipper to the highest bidder as part of the process. Finally, as more and more companies use blockchain, there will be a proliferation of smart contract templates available for use. Tools for finding templates appropriate for a given style of collaboration will be essential. All these characteristics emphasize the need for specific testing and verification approaches. Execution refers to the instantiation of individual cases and their information-technological processing. Currently, such execution is facilitated by process-aware information systems or digital economy process management systems. For the actual execution of a process deployed on a blockchain following the method of (Mendling, 2018), several differences with the traditional ways exist.

During the execution of an instance, messages between participants need to be passed as blockchain transactions to the smart contract; resulting messages need to be observed from the blocks in the blockchain. Both of these can be achieved by integrating blockchain technology directly with existing enterprise systems or through the use of dedicated integration components, such as the triggers suggested by (Mendling, 2018). The main challenge here involves ensuring correctness and security, especially when monetary assets are transferred using this technology. Process monitoring refers to collecting events of process executions, displaying them in an understandable way, and triggering alerts and escalation in cases where undesired behavior is observed.

Currently, such process execution data is recorded by systems that support process execution (Mendling, 2018). *First*, we face issues in terms of data fragmentation and encryption as in the analysis phase. For example, the data on the blockchain alone will likely not be enough to monitor the process, but require integration with local off-chain data. Once such tracing in place, the global view of the process can be monitored independently by each involved party. This provides a suitable basis for continuous conformance and compliance checking and monitoring of service-level agreements. *Second*, based on monitoring data exchanged via the blockchain, it is possible to verify if a process instance meets the original process model and the contractual obligations of all involved process stakeholders. For this, blockchain technology can be exploited to store the process execution data and handoffs between process participants. Notably, this is even possible without the usage of smart contracts, i.e., in a first-generation blockchain like the one operated by digital economy.

Runtime adaptation refers to the concept of changing the process during execution. In traditional approaches, this can for instance be achieved by allowing participants in a process to change the model during its execution. Interacting partners might take a defensive stance in order to avoid certain types of adaptation. As discussed by (Mendling, 2018), blockchain can be used to enforce conformance with the model, so that participants can rely on the joint model being followed. In such a setting, adaptation is by default something to be avoided: if a participant can change the model, this could be used to gain an unfair advantage over the other participants. For instance, the rules of retrieving digital process from an escrow account could be changed or the terms of payment. In this setting, process adaptation

must strictly adhere to defined paths for it, e.g., any change to a deployed smart contract may require a transaction signed by all participants.

In contrast, the method proposed by Mendling et al. (*Mendling, 2018*) allows runtime adaptation, but assumes that relevant participants monitor the execution and react if a change is undesired. If smart contracts enforce the process, there are also problems arising in relation to evolution: new smart contracts need to be deployed to reflect changes to a new version of the process model. Porting running instances from an old version to a new one would require effective coordination mechanisms involving all participants.

There are also challenges and opportunities for digital economy process and blockchain technology beyond the classical lifecycle. We refer to the capability areas beyond the methodological support we reflected above, including strategy, governance, information technology, people, and culture. Strategic alignment refers to the active management of connections between organizational priorities and business processes, which aims at facilitating effective actions to improve business performance. Currently, various approaches to digital economy process assume that the corporate strategy is defined first and business processes are aligned with the respective strategic imperatives (*Mendling, 2018*). Blockchain technology challenges these approaches to strategic alignment. For many companies, blockchains define a potential threat to their core digital economy processes. For instance, the banking industry could see a major disintermediation based on blockchain-based payment services. Also lock-in effects might deteriorate when, for example, the banking service is not the banking network itself anymore, but only the interface to it. These developments could lead to business processes and business models being under strong influence of technological innovations outside of companies (Mkrttchian, et. al, 2019).

The digital economy process governance refers to appropriate and transparent accountability in terms of roles, responsibilities, and decision processes for different digital economy-related programs, projects, and operations. Currently, digital economy processes as a management approach builds on the explicit definition of digital economy processes management-related roles and responsibilities with a focus on the internal operations of a company. Blockchain technology might change governance towards a more externally oriented model of self-governance based on smart contracts. Research on corporate governance investigates agency problems and mechanisms to provide effective incentives for intended behavior (*Mendling, 2018*).

Smart contracts can be used to establish new governance models as exemplified by Mendling et al. (2018). It is an important question in how far this idea of Mendling can be extended towards reducing the agency problem of management discretion or eventually eliminate the need for management altogether. Furthermore, the revolutionary change suggested by Mendling, for organization shows just how disruptive this technology can be, and whether similarly radical changes could apply to digital economy processes management (*Mendling, 2018*).

Digital economy processes management-related information technology subsumes all systems that support process execution, such as process-aware information systems and digital economy process management systems. These systems typically assume central control over the process. Blockchain technology enables novel ways of process execution, but several challenges in terms of security and privacy have to be considered. While the visibility of encrypted data on a blockchain is restricted, it is up to the participants in the process to ensure that these mechanisms are used according to their confidentiality requirements. Some of these requirements are currently being investigated in the financial industry. Further challenges can be expected with the introduction of the digital economy in Russian Federation. It is also not clear, which new attack scenarios on blockchain networks might emerge. Therefore, guidelines for using private, public, or consortium-based blockchains are required.

A person in this context refers to all individuals, possibly in different roles, who engage with digital economy processes management. Currently, these are people who work as process analyst, process manager, process owner or in other process-related roles. The roles of these individuals are shaped by skills in the area of management, business analysis and requirements engineering. In this capability area, the use of blockchain technology requires extensions of their skill sets. New required skills relate to partner and contract management, software engineering and big data analysts. Also, people have to be willing to design blockchain-based collaborations within the frame of existing regulations to enable adoption. This implies that research into blockchain-specific technology acceptance is needed, extending the established technology acceptance model (*Mendling, 2018*).

Organizational culture is defined by the collective values of a group of people in an organization. Currently, digital economy processes management is discussed in relation to organizational culture from a perspective that emphasizes an affinity with clan and hierarchy culture. These cultural types are often found in the many companies that use digital economy processes management as an approach for documentation. Blockchains are likely to influence organizational culture towards a stronger emphasis on flexibility and an outward-looking perspective. In the competing values framework by Mendling et al. (2018), these aspects are associated with an adhocracy organizational culture. Furthermore, not only consequences of blockchain adoption have to be studied, but also antecedents'. These include organizational factors that facilitate early and successful adoption (*Mkrttchian, et. al, 2019*).

By itself, stored data does not generate business value, and this is true of traditional databases, data warehouses, and the new technologies for storing big data. Once the data is appropriately stored, however, it can be analyzed, which can create tremendous value. A variety of analysis technologies, approaches, and products have emerged that are especially applicable to big data, such as in-memory analytics, in-database analytics, and appliances. In our study we are using Intelligent Visualization Techniques for Big Data Analytic, or business intelligence (*Mkrttchian and Aleshina, 2017; Plotnikov, 2016; Mkrttchian, 2011; Mkrttchian, 2012 and other*).

It is helpful to recognize that the term analytics is not used consistently; it is used in at least three different yet related ways. A starting point for understanding analytics is to explore its roots. Decision support systems (DSS) in the 1970s were the first systems to support decision making. DSS came to be used as a description for an application and an academic discipline. Over time, additional decision support applications such as executive information systems, online analytical processing (OLAP), and dashboards/scorecards became popular (*Watson and Hugh, 2014*).

Descriptive analytics, such as reporting/OLAP, dashboards/scorecards, and data visualization, have been widely used for some time, and are the core applications of traditional BI. Descriptive analytics are backward looking (like a car's rear view mirror) and reveal what has occurred. One trend, however, is to include the findings from predictive analytics, such as forecasts of future sales, on dashboards/scorecards (*Watson and Hugh, 2014*).

The methods and algorithms for predictive analytics such as regression analysis, machine learning, and neural networks have existed for some time. Recently, however, software products such as SAS Enterprise Miner have made them much easier to understand and use. They have also been integrated into specific applications, such as for campaign management. Marketing is the target for many predictive analytics applications; here the goal is to better understand customers and their needs and preferences.

Some people also refer to exploratory or discovery analytics, although these are just other names for predictive analytics. When these terms are used, they normally refer to finding relationships in big data that were not previously known. The ability to analyze new data sources—that is, big data—creates additional opportunities for insights and is especially important for firms with massive amounts of

customer data. Golden path analysis is a new and interesting predictive or discovery analytics technique. It involves the analysis of large quantities of behavioral data (i.e., data associated with the activities or actions of people) to identify patterns of events or activities that foretell customer actions such as not renewing a cell phone contract, closing a checking account, or abandoning an electronic shopping cart. When a company can predict a behavior, it can intercede, perhaps with an offer, and possibly change the anticipated behavior (Watson and Hugh, 2014).

There is no formula for choosing the right platforms. However, the most important considerations include the volume, velocity, and variety of data; the applications that will use the platform; that the users are; and whether the required processing is batch or real time. Some work may require the integrated use of multiple platforms. The final choices ultimately come down to where the required work can be done at the lowest cost. For our goal is good Triple H Avatar an Avatar-based Software Platform for HHH University, Sydney, Australia.

CONCLUSION

Blockchain will fundamentally shift how we deal with transactions in general, and therefore how organizations manage their business processes within their network. Discussion of challenges in relation to the digital economy processes management lifecycle and beyond points to seven major future research directions. For some of them we expect viable insights to emerge sooner, for others later. The order loosely reflects how soon such insights might appear. The digital economy processes management and the Information Systems community have a unique opportunity to help shape this fundamental shift towards a distributed, trustworthy infrastructure to promote inter-organizational processes.

ACKNOWLEDGMENT

The reported study was funded by RFBR according to the research project No. 18-010-00204_a.

REFERENCES

- Calvão, F. (2018). Crypto-miners: Digital labor and the power of blockchain technology. *Economic Anthropology*, 6(1), 123–134. doi:10.1002/ea.2.12136
- Cayoglu, U. (2014). *Report: The Process Model Matching Contest 2013. In BPM 2013: Business Process Management Workshops* (pp. 442–463). Springer.
- Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. (2013). *Fundamentals of Business Process Management*. Springer. doi:10.1007/978-3-642-33143-5
- Epler, P. (2013). Using the Response to Intervention (RtI) Service Delivery Model in Middle and High Schools. *International Journal for Cross-Disciplinary Subjects in Education*, 4(1), 1089–1098. doi:10.20533/ijcdse.2042.6364.2013.0154
- Euzenat, J., & Shvaiko, P. (2013). Ontology Matching: State of the Art and Future Challenges. *IEEE Transactions on Knowledge and Data Engineering*, 25(1), 158–176. doi:10.1109/TKDE.2011.253

Hegadekatti, K. (2017). *Blockchain Technology - An Instrument of Economic Evolution?* SSRN Electronic Journal. doi:10.2139/ssrn.2943960

Khan, M. S., Ferens, K., & Kinsner, W. (2014). A Chaotic Complexity Measure for Cognitive Machine Classification of Cyber-Attacks on Computer Networks. *International Journal of Cognitive Informatics and Natural Intelligence*, 8(3), 45–69. doi:10.4018/IJCINI.2014070104

Mendling, J. (2018). Blockchains for Business Process Management – Challenges and Opportunities. *ACM Trans. Manag. Inform. Syst.*, 9.

Mkrttchian, V. (2011). Use ‘hhh’ technology in transformative models of online education. In G. Kurubacak & T. Vokan Yuzer (Eds.), *Handbook of research on transformative online education and liberation: Models for social equality* (pp. 340–351). Hershey, PA: IGI Global. doi:10.4018/978-1-60960-046-4.ch018

Mkrttchian, V. (2012). Avatar manager and student reflective conversations as the base for describing meta-communication model. In G. Kurubacak, T. Vokan Yuzer, & U. Demiray (Eds.), *Meta-communication for reflective online conversations: Models for distance education* (pp. 340–351). Hershey, PA: IGI Global. doi:10.4018/978-1-61350-071-2.ch005

Mkrttchian, V. (2015). Modeling using of Triple H-Avatar Technology in online Multi-Cloud Platform Lab. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3rd ed.; pp. 4162-4170). Hershey, PA: IGI Global. Doi:10.4018/978-1-4666-5888-2.ch409

Mkrttchian, V., & Aleshina, E. (2017). *Sliding Mode in Intellectual Control and Communication: Emerging Research and Opportunities*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2292-8

Mkrttchian, V., Bershadsky, A., Bozhday, A., & Fionova, L. (2015). Model in SM of DEE Based on Service Oriented Interactions at Dynamic Software Product Lines. In G. Eby & T. Vokan Yuzer (Eds.), *Identification, Evaluation, and Perceptions of Distance Education Experts* (pp. 230–247). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8119-4.ch014

Mkrttchian, V., Bershadsky, A., Bozhday, A., Kataev, M., & Kataev, S. (Eds.). (2016). *Handbook of Research on Estimation and Control Techniques in E-Learning systems*. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-9489-7

Mkrttchian, V., Gamidullaeva, L. A., Vertakova, Y., & Panasenko, S. (2019). New Tools for Cyber Security Using Blockchain Technology and Avatar-Based Management Technique. In M. Khan (Ed.), *Machine Learning and Cognitive Science Applications in Cyber Security* (pp. 105–122). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-8100-0.ch004

Mkrttchian, V., Kataev, M., Hwang, W., Bedi, S., & Fedotova, A. (2014). Using Plug-Avatars “hhh” Technology Education as Service-Oriented Virtual Learning Environment in Sliding Mode. In G. Eby & T. Vokan Yuzer (Eds.), *Emerging Priorities and Trends in Distance Education: Communication, Pedagogy, and Technology*. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-5162-3.ch004

Mkrttchian, V., Kataev, M., Hwang, W., Bedi, S., & Fedotova, A. (2016). Using Plug-Avatars “hhh” Technology Education as Service-Oriented Virtual Learning Environment in Sliding Mode. In *Leadership and Personnel Management: Concepts, Methodologies, Tools, and Applications* (pp. 890-902). Hershey, PA: IGI Global. Doi:10.4018/978-1-4666-9624-2.ch039

- Morabito, V. (2017a). Blockchain and Enterprise Systems. *Business Innovation Through Blockchain*, 125–142. doi:10.1007/978-3-319-48478-5_7
- Morabito, V. (2017b). The Blockchain Paradigm Change Structure. *Business Innovation Through Blockchain*, 3–20. doi:10.1007/978-3-319-48478-5_1
- Morabito, V. (2017c). Blockchain Practices. *Business Innovation through Blockchain*, 145–166. doi:10.1007/978-3-319-48478-5_8
- Plotnikov, V., Vertakova, Y., & Leontyev, E. (2016). Evaluation of the effectiveness of the telecommunication company's cluster management. *Economic Computation and Economic Cybernetics Studies and Research*, 50(4), 109–118.
- Swan, M. (2018). Blockchain Economic Networks: Economic Network Theory—Systemic Risk and Blockchain Technology. *Business Transformation through Blockchain*, 3–45. doi:10.1007/978-3-319-98911-2_1
- Tran, T. P., Tsai, P., Jan, T., & He, X. (2012). Machine Learning Techniques for Network Intrusion Detection. In I. Management Association (Ed.), *Machine Learning: Concepts, Methodologies, Tools and Applications* (pp. 498–521). Hershey, PA: IGI Global. doi:10.4018/978-1-60960-818-7.ch310
- Van der Aalst, W. M. P. (2016). *Process Mining: Data Science in Action*. Springer. doi:10.1007/978-3-662-49851-4
- Watson, H. J. (2014). Tutorial: Big Data Analytics: Concepts, Technologies, and Applications. *Communications of the Association for Information Systems*, 34, 65. doi:10.17705/1CAIS.03465

ADDITIONAL READING

- Glотова, T., Deev, M., Krevskiy, I., Matukin, S., Mkrttchian, V., & Sheremeteva, E. (2015). Individualized learning trajectories using distance education technologies, In A. Kravets, M. Shcherbakov, M. Kultsova, & O. Shabalina, (Eds.), *Proceedings of CIT&DS 2015*, (pp. 778–793). Switzerland: Springer International Publishing AG. DOI: 10.1007/978-3-319-23766-4
- Mkrttchian, V. (2016). The Control of Didactics of Online Training of Teachers in HHH University and Cooperation with the Ministry of Diaspora of Armenia. In V. Mkrttchian, A. Bershadsky, A. Bozhday, M. Kataev, & S. Kataev (Eds.), *Handbook of Research on Estimation and Control Techniques in E-learning systems* (pp. 311–322). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-4666-9489-7.ch021
- Mkrttchian, V., & Belyanina, L. (2016). The Pedagogical and Engineering Features of E- and Blended Learning of Adults Using Triple H-Avatar in Russian Federation. In V. Mkrttchian, A. Bershadsky, A. Bozhday, M. Kataev, & S. Kataev (Eds.), *Handbook of Research on Estimation and Control Techniques in E-Learning Systems* (pp. 61–77). Hershey, PA, USA: IGI Global; doi:10.4018/978-1-4666-9489-7.ch006

KEY TERMS AND DEFINITIONS

Audit and Policy Mechanisms: Is a section of avatar-based management techniques.

Avatar-Based Management: Is control methods and techniques introduced by V. Mkrttchian in 2018.

Blockchain: Is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block a timestamp, and transaction data.

Cyber Security: Is section of information security, within the framework of which the processes of formation, functioning and evolution of cyber objects are studied, to identify sources of cyber-danger formed while determining their characteristics, as well as their classification and formation of regulatory documents, implementation of security systems in future.

Machine Learning Application: Is class of methods of artificial/natural intelligence, the characteristic feature of which is not a direct solution of the problem but training in the process of applying solutions to a set of similar problems.

Maturity Models: Is a section of avatar-based management.

Predictive Analytics: Is the use of data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on empirical data.

An Overview (and Criticism) of Methods to Detect Fake Content Online

Antonio Badia

University of Louisville, USA

INTRODUCTION

The Web facilitates the spread of information thanks to its interconnected nature and the ease of publishing on it; but there seems to be lately a drastic increase in content of doubtful veracity (Kumar and Shah, 2018). Given the use of the Web as a diffusion media (60% of Americans get their news from social media, according to (Allcott et al, 2017)), this has become an important issue. In the Web, it is relatively easy to produce content that maximizes dissemination (achieves ‘virality’) by using attention-calling techniques (like clickbait) that take advantage of recommendation algorithms. As a result, there is a process of ‘algorithmic amplification’ of fake content (DiResta, 2018).

This has produced alarm, as false and misleading information is reaching wide audiences and doing it faster than truthful, accurate content (Shao et alia, 2018; Hui et alia, 2018). Therefore, there is much interest in the research community (and society at large) in detecting certain forms of fake content and eliminating (or at least restricting) its diffusion.

In this chapter, we provide an overview of recent algorithmic approaches to detecting fake content. This is a very active and ongoing area of work; we will not offer a comprehensive review of all relevant research, rather offering a representative sample. The thesis of this chapter is that such research is characterized by a very narrow scope and a lack of definition of its target (i.e. what exactly is fake content?). To support this thesis, we first examine the concept and show that it is a multi-faceted, complex phenomena; hence, it is very difficult to agree on an exact definition of what constitutes falsehood. As a result, most research has focused on a narrow subset of the topic (usually called fact checking). Next, we summarize research efforts to detecting fake content, and provide a brief evaluation of the state of the art. Finally, we sketch some suggestions for future research, emphasizing that this is still an open problem and that further work will require a better approach to defining fake content and its various aspects.

We do not cover other, closely related aspects of the problem, like legal, political and criminal approaches to defining, detecting and fighting fake content. Such aspects are very interesting and relevant, but deserve a chapter of their own. Rather, we assume that technological efforts to detect false content are an important tool that can be used by these other approaches, but to do so it must evolve past current attempts.

BACKGROUND: DEFINING FAKE CONTENT

One of the most challenging aspects of the research about fake content is the difficulty of defining the concept. There is much disagreement among authors; while the idea of being ‘true’ or ‘false’ has a strong intuitive sense, there is a lack of formal definitions that are widely shared. A considerable amount of work does not formally define ‘fake’ or ‘false’ (or, equivalently, ‘true’ or ‘truth’). Thus, ad-hoc defini-

DOI: 10.4018/978-1-5225-9715-5.ch072

tions are used in many cases (Shu et al., 2017). For instance, a Stanford study on misinformation uses a set of fake content obtained by combining articles from the PolitiFact web site, the BuzzFeed website, and two previous academic articles (Allcott et al., 2019). It classifies as fake news any post from a short list of sites which are ‘well known to be providers of false information.’ To make the issue even more complicated, there are a number of related concepts (fake reviews, clickbait, rumors, hate speech, cognitive hacking) that tend to get confused (that is why this article uses the more neutral label ‘fake content’ (Tandoc et al., 2017)).

An area that has looked in depth at the problem of true or authentic information is that of Intelligence studies; this area provides a starting point for trying to define false news (Hansen, 2017). Based on this work, we can distinguish the following aspects:

- **‘Fake’ as ‘Non-Factual’:** This refers to statements describing events or facts that are considered not to be a faithful representation of what happens in the real world. Many studies implicitly use this idea; for instance, “Fake news is an article that is intentionally and verifiably false.” (Shu et al., 2017, p. 23). Note that this approach requires the existence of some ground truth that can be objectively assessed; this is easy in some cases (location of a store, hours it is open) but not so in others. Factual statements may involve several aspects:
 - Factual concrete information, that is, about a particular event or action. The falsehood usually refers to describing an event that did not happen, and denying the occurrence of an event that did happen. Most research in fake content focuses on this aspect of the issue.
 - **Factual General Information:** This refers to general or scientific knowledge. An example of this is how medical knowledge is distorted by many pseudo-scientific theories that proliferate on the Web, like anti-vaccine beliefs. Another example is climate change denial. There is a debate as to whether these platforms actively contribute to maximize the impact of this pseudo-information, due to their algorithms (DiResta, 2018).
- **‘Fake’ as ‘Incomplete/Misleading’:** For complex events or actions, an accurate and complete description may involve complex statements. A partial description presenting carefully selected aspects, with each aspect factually true, may create a false impression: “omitted facts or untold stories which, if viewed by the standard of traditional editorial guidelines, would definitely have been considered newsworthy.” (Hanson, 2017, p. 21). This is usually achieved by suppressing some relevant aspects and/or highlighting barely meaningful ones, and can be considered a falsehood in the sense that the significance or interpretation of the event or action in a larger context is completely hidden.
- **‘Fake’ as ‘Biased’:** The description is done from one perspective only, resulting in a slanted view of the event or action: “the reporting may be so one-sided as to disqualify it. It may not necessarily contain untruths, but it is done less to inform than to leave the news consumer with a certain set of emotions and, ultimately, with certain political preferences.” (Hanson, 2017, p. 21). Note that, different from the previous case, where each individual statement was truthful but the collection was not, here the individual statements (whether there is only one or several) are distorted.
- **‘Fake’ as ‘Opinion’:** This refers to non-factual information: opinion, commentary on news, and similar. This is the most ambiguous area, since it is assumed that when someone gives an opinion, the speaker is not bound to be objective. This area includes speech which is conflictive for other reasons, like hate speech; however, given its ambiguity, hate speech is usually not considered a target for fake content detection, with a few specific exceptions: in e-commerce, *fake reviews* is

a significant problem (Mukherjee et alia, 2013). While there is also research on detecting hate speech (Gröndahl et alia, 2018), it will not be covered in this article.

There are other possible classifications of fake content. For instance, (Tandoc et alia, 2017) propose a typology using 2 dimensions: the degree of facticity, and the intention to deceive. (Wardle 2017) proposes 3 dimensions: the type of content, the motivation(s) of the creator(s), and the way the content is disseminated. Another classification is based on the origin of the content:

- **Generated by a Person:** this can be further subdivided into user generated content (fake reviews, mostly) and professional generated content (fake news, when written by a group of professional writers, usually under the auspices of some organization, in order to generate and adversarial setting).
- **Generated by Machine:** This can refer to reviews or news; the distinctive feature is that they are generated by algorithm. The goal here is to extend the reach of fake content by generating a large amount of such content and spreading it widely.

An important (but orthogonal) issue is that of intentionality. Usually, a distinction between ‘misinformation’ and ‘disinformation’ is made in this context. Disinformation is taken to refer to “information which is known to be untrue or even deliberately fabricated. It is intentionally false.” while disinformation refers to situations where the source is unaware that the information is false. Note that the same statement may fall under both cases, depending on the context: “If [disinformation] is subsequently spread by someone who is unaware of its false nature, it is reduced to misinformation. (The term “fake news” seems to include both disinformation and misinformation.)” (Hansen, 2017, p. 21). This aspect is important in certain fields, for instance legal: “For purposes of this article, we define “fake news” as the online publication of intentionally or knowingly false statements of fact.” (Klein and Wueller, 2017). However, here we do not consider this issue, as most algorithmic approaches also disregard this aspect.

There are other notions closely related to ‘falsehood’ but different from it. The term “cognitive hacking” refers to the manipulating public opinion for de-stabilizing efforts like stock market manipulation, attacking media credibility, etc. It can be achieved by any of the aspects described above. Some authors argue that, while many approaches try to establish the credibility of sources, truth is different from credibility: credibility can be considered a subjective property; in communication, receiver and sender may disagree on issues of credibility (Wierzbicki, 2018). Controversial information is that for which there is a disagreement in credibility.

Finally, and even though most approaches reviewed here focus on text, fake content is not always expressed textually. The production of non-truthful content can be extended to other media: deep fakes are the equivalent of fake content in multimedia (video, audio and images).

APPROACHES TO DETECTION

There are two basic approaches to detecting fake content: human based and computational. We describe each one in turn.

Human-Based Approaches

Human-based approaches, like their name indicates, are ultimately based on a person's identification of discrepancies between what a message says and established facts ('manual fact checking'). Since this approach is labor intensive, and there is an element of individual judgment that may bias the results, this is usually a team effort. This approach has been used by Facebook, Twitter and other companies due to the limitations of current computational approaches (see below).

Human-based efforts usually depend on curated sources. There have been several projects to identify and gather collections of trustable sources. The WOT system¹ uses crowdsourcing to determine if a web site is credible. However, crowdsourcing may be manipulated using *astroturfing*, the practice of making a message appear as if originated by a 'grassroots' movement and hiding the real originator. Snopes² focuses on evaluating urban legends. Politifact³ deals with statements made by politicians and other people with authority. It uses a team of experts (journalists). Evaluations result in ratings, which are usually accompanied by detailed explanations of the rating. FactCheck.org⁴ focuses on statements by politicians and also relies on journalists. The Stanford Web Credibility Project⁵ focuses more on how users evaluate the credibility of Web resources.

Human-based approaches have severe limitations. First, the approaches used at Internet companies like Facebook are not public and therefore it is not known what guidelines the humans use or what definition of fake information is used, or how it is detected. This has led to a variety of groups claiming discrimination by the company. Second, the human approach depends on a person's judgment and this involves the risk of biased, incomplete or even inconsistent results (Lim, 2018). Finally, this approach does not scale to Internet size, and therefore is it unlikely to be a long-term solution.

Algorithmic Approaches

The problems of human-based approaches has led to interest in computational approaches. These approaches can, in turn, be divided into three broad classes: knowledge-based, diffusion-based, and content-based.

Knowledge-based approaches compare the content of a message with established ground truth collected on knowledge bases like DBpedia (Ciampaglia et al., 2105; Shi and Weninger, 2016). The main challenges to these approaches are twofold. First, they depend on the coverage of the knowledge base, which can be quite limited in certain domains. Second, it can be very difficult to detect subtle contradictions in two pieces of text (Marneffe et al., 2018).

Approaches based on diffusion are mainly applied to Web content, since in this environment it is usually possible to trace the spread of content (and sometimes its lineage, ie where it originated and how it was transmitted). It is claimed that false content disseminates in a manner different from truthful content, and hence can be detected by examining patterns of diffusion (Shao et alia, 2016; Hui et alia, 2018, Vosoughi et alia, 2018). These approaches have been successful in detecting hoaxes, fake reviews and spam (Tachini et alia, 2017; Zin et alia, 2016). However, many of them examine patterns of diffusion and therefore only help to detect fake news after they have reached many users.

Content-based approaches are usually based on Machine Learning techniques, in particular, Supervised Machine Learning. In this approach, training data (usually, collections of news articles) are described by a set of attributes or *features* and labeled (classified as 'fake' or 'real'). A Machine Learning algorithm is fed the training data and it attempts to learn a model, which identifies patterns in the data connecting the features with the labels. The model is then fed new, unlabeled news articles and is able to determine whether they are 'fake' or 'real'. The set of features used varies per approach, but it usually includes

lexical features (the presence or absence of certain words, the style in which a document is written, number of spelling mistakes, presence or absence of quotes, etc.), although sometimes additional features (information about the source) are also used. For instance, for clickbait detection, it is common to include the token similarity between title and text and the existence of certain Part Of Speech (POS) patterns (Chen, Conroy and Rubin, 2015a). Sometimes, specific patterns are found to work in certain domains, like the use of satirical language in fake news production (Chen, Conroy and Rubin, 2016).

Some computational approaches have achieved good results, albeit in limited domains. For instance, clickbait detection has been shown to be a bit easier than fake content detection, thanks the characteristics of clickbait: an attention-gathering title or headline that has a weak connection with the content of the article (Chen, Conroy and Rubin, 2015b) plus repetitions in the content (Horne and Adali, 2017).

Algorithmic approaches are hard to evaluate because there are not widely recognized benchmarks for fake news detection, and not widely agreed-upon method to determine accuracy; as a result, each group of researchers uses their own dataset.

Evaluation

Algorithmic approaches to fake news detection have some common characteristics. First, they limit themselves to dealing with factual (concrete) information and do not deal with more complex scenarios. In particular, misleading or biased information is beyond the scope of most approaches. Second, many approaches do not attempt to actually check the content of the messages or text they deal with: they instead rely on diffusion patterns (when dealing with messages on social networks (Shao et al., 2016)) or on lexical and syntactic features of the text (Yang and Nenkova, 2017). Third, no approach has a clear, explicit definition of what being fake is. In this regard, it is important to point out that Machine Learning approaches do not have an explicit definition of fake, but do use an implicit definition: such a characterization comes from their labeled dataset. In essence, the set of messages or texts that are marked as ‘fake’ constitute an implicit definition.

As a result of these characteristics, even state-of-the-art algorithms have serious limitations: those based on network dissemination only apply to social media, and determine truthfulness a posteriori, after the message has spread, thereby not being useful for prevention. Those based on content work better when the content is limited to a certain style, like clickbait, that provide strong structural clues. All computational approaches are very hard to evaluate as there are no widely adopted benchmarks. On top of the current limited effectiveness, some new research has shown that such tools are not difficult to fool (Grondahl et al. 2018).

FUTURE RESEARCH DIRECTIONS

As should be clear from this overview, detecting fake content is an open problem. There is no wide agreement on what constitutes the target concept, which in turn makes it very difficult to create widely shared and used benchmarks. In particular, for approaches that depend on deep learning, the creation of labeled data sets for training is highly problematic. It is known, from past experience, that extreme care is needed when creating training sets, since most algorithms will pick any bias, intentional or unintentional, in the training data (O’Neil, 2014; Noble, 2018). The importance of this problem is reflected on the nascent field of Algorithmic Fairness (Sun et alia, 2018). Thus, it is urgent that researchers agree on an acceptable definition of what is ‘fake content’ and that shareable benchmarks are developed. Also,

labeled datasets for training would be very desirable for approaches based on Supervised Machine Learning. While a few already exist, they have not gained widespread usage (Vlachos and Riedel, 2014).

Some authors have argued that the problem has no algorithmic solution and that social, legal and organizational approaches are needed. While it is clear that fake content does require a concerned effort on all these fronts, computational approaches are absolutely needed in order to push back against the Internet scale of the problem. This is not to say that other approaches cannot help; for instance, finding a way to reduce the incentives (monetary and otherwise) to produce fake news would go a long way towards solving the problem. At the same time, any said solutions must be developed with care; simply leaving control of what is and is not shareable (what constitutes fake content, spam, hate speech and so on) to a few companies may devolve into censorship and biases. Thus, this is an issue that should involve society at large.

CONCLUSION

Fake content generation and distribution on the Web is a very important problem, perhaps the top problem in the Web nowadays due to its repercussions. In spite of this, it has been only recently that researchers and institutions have started spending a substantial amount of effort to combat it. The problem is still open and is the subject of very active research.

Both human-based and computation-based approaches have been proposed. Unfortunately, both types have significant drawbacks. On the computational side, the lack of agreement on exactly what constitutes false content has resulted in a lack of standardized benchmarks to evaluate research, and in difficulty to develop labeled data for Supervised Machine Learning approaches.

One important aspect is the role that social networks themselves play in the diffusion of false content. As seen above, a considerable body of research argues that this content disseminates faster and wider than truthful content. Reluctance to control content has also make the situation more problematic.

In the future, we can expect to see more Machine Learning models being developed, as more and better labeled datasets become available, and more features are included. We can also expect to see other solutions besides purely technical ones; the study by Hansen “suggests to focus on the build-up of greater cognitive resilience, that is, the ability to withstand pressure from various ideas spread, for instance, through disinformation.” (Hansen, 2017, p. 35) The idea is to make individuals immune to contagion by making them not believe such news: “In essence, it will allow for the free flow of information, including from Russian state-controlled media, but it will establish a cognitive ‘firewall’, which prevents the disinformation from taking root and being internalized by members of the target audience.” (Hansen, 2017, p. 35) This is not a technical, even business-based, solution: the firewall should work at the institutional and personal level. That is, the whole population should be involved; this is to be achieved by education -providing everyone with media literacy (Hanson, 2017), the ability to examine critically pieces of information and tell fake news from real ones.

REFERENCES

- Alcott, H., & Getznkow, M. (2017). Social Media and Fake News in the 2016 Election. *The Journal of Economic Perspectives*, 31(2), 211–236. doi:10.1257/jep.31.2.211
- Allcott, H., Getznkow, M., & Yu, C. (2019). *Trends in the diffusion of misinformation on social media*. Research & Politics. doi:10.3386/w25500
- Ciampaglia, G., Shiralkar, P., Rocha, L., Bollen, J., Menzer, F., & Flammini, A. (2015). Computational Fact Checking from Knowledge Networks. *PLoS One*, 10(6), e0128193. doi:10.1371/journal.pone.0128193 PMID:26083336
- Conroy, N., Rubin, V., & Chen, Y. (2015a). Automatic deception detection: Methods for finding fake news. *Proceedings of the Association for Information Science Technology*, 52(1), 1–4. doi:10.1002/pra2.2015.145052010082
- Conroy, N., Rubin, V., & Chen, Y. (2015b). Misleading online content: recognizing clickbait as false news. *Proceedings Of the ACM Workshop on Multimodal Deception Detection*, 15-19.
- Conroy, N., Rubin, V., & Chen, Y. (2016). Fake News or truth? Using satirical cues to detect potentially misleading news. *Proceedings Of the 2nd Workshop on Computational Approaches to Deception Detection*, 7-17.
- DiResta, R. (2018). *Free Speech Is Not the Same As Free Reach*. Retrieved from <https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/>
- Gröndahl, T., Pajola, L., Juuti, M., Conti, M., & Asokan, N. (2018). *All You Need is Love: Evading Hate-speech Detection*. Retrieved from <https://arxiv.org/abs/1808.09115v1>
- Hansen, F. (2017). *Russian Hybrid Warfare: A study of Disinformation*. Danish Institute for International Studies (DIIS) Technical Report.
- Horne, B. & Adali, S. (2017). *This just in: fake news pack a lot in title, uses simple, repetitive content in text body, more similar to satire than real news*. ArXiv, 1703.09398
- Jin, Z., Cao, J., Zhang, Y., & Luo, J. (2016). News verification by exploiting conflicting social viewpoints in microblogs. In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*. AAAI Press.
- Klein, D., & Wueller, J. (2017). *Fake News: A Legal Perspective*. Retrieved from <http://www.kleinmoynihan.com/fake-news-a-legal-perspective/>
- Kumar, S., & Shah, N. (2018). *False Information on Web and Social Media: A Survey*. Retrieved from <https://arxiv.org/abs/1804.08559>
- Lim, C. (2018). *Checking how fact-checkers check*. Research & Politics. doi:10.1177/2053168018786848
- Marneffe, M., Rafferty, A., & Manning, C. (2008) Finding contradictions in text. *Proceedings of ACL-08: HLT*, 1039-1047.
- Murkhejee, A., Liu, B., & Glance, N. (2013) Spotting fake reviewer groups in consumer reviews. In *Proceedings of the 21st International Conference on the World Wide Web*. ACM.

- Noble, S. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: New York University Press. doi:10.2307/j.ctt1pwt9w5
- O'Neil, C. (2016). *Weapons of Math Destruction*. Washington, DC: Crown Books.
- Perez-Rosas, V., Kleinberg, B., Lefevre, A., & Mihalcea, R. (2018). Automatic Detection of Fake News. In *Proceedings of the 27th International Conference on Computational Linguistics*. ACM.
- Shao, C., Ciampaglia, G., Flammini, A., & Menczer, F. (2016). Hoaxy: A Platform for Tracking Online Misinformation. *Proceedings of the 25th International Conference Companion on World Wide Web*, 745–750. 10.1145/2872518.2890098
- Shao, C., Hui, P., Wang, L., Jiang, X., Flammini, A., Menczer, F., & Ciampaglia, G. (2018). Anatomy of an online misinformation network. *PLoS One*, 13(4), 1–23. doi:10.1371/journal.pone.0196087 PMID:29702657
- Shi, B., & Wenginger, T. (2016). *Fact Checking in Heterogeneous Information Networks*. doi:10.1145/2872518.2889354
- Shu, K., Sliva, A., Wang, S., Tang, J. & Liu, H. (2017). Fake News Detection on Social Media: a data mining perspective. *ACM SIGKDD Explorations Newsletter*, 19(1).
- Sun, W., Nasraoui, O., & Shafto, P. (2018). Iterated Algorithmic Bias in the Interactive Machine Learning Process of Information Filtering. In *Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. Seville, Spain: SCITEPRESS - Science and Technology Publications. 10.5220/0006938301100118
- Tachini, E., Ballarin, G., Vedova, M., Moret, S., & de Alfaro, L. (2017). *Some Like it Hoax: automated fake news detection in social networks*. arXiv preprint: 1704.07506
- Tandoc, E., Lim, Z., & Ling, R. (2017). Defining “fake news” a typology of scholarly definitions. *Digital Journal*, 6, 1–17.
- Vlachos, A., & Riedel, S. (2014). Fact Cheching: task definition and dataset construction. *Proceedings of the ACL Workshop on Language Technologies and Computational Social Science*, 18–22. 10.3115/v1/W14-2508
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Nature*, 359(6380), 1146–1151. PMID:29590045
- Wardle, C. (2017). *Fake News. It's Complicated*. Retrieved from <https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79>
- Wierzbicki, A. (2018). *Web Content Credibility*. Springer. doi:10.1007/978-3-319-77794-8
- Yang, Y., & Nenkova, A. (2017, September). Combining lexical and syntactic features for detecting content-dense texts in news. *Journal of Artificial Intelligence Research*, 60(1), 179–219. doi:10.1613/jair.5418

KEY TERMS AND DEFINITIONS

5

Clickbait: Web article with an attention-gathering headline designed to make users click on the link, but with content rarely connected to the headline at all.

Crowdsourcing: The practice of hiring a (large) group of people (the ‘crowd’) to accomplish a certain task, usually a repetitive task that does not require special training but that must be carried out over a large amount of data.

Disinformation: False content that is deliberately fabricated and distributed.

Fake News: False content that tries to appear as coming from a traditional news media outlet.

Fake Reviews: Product review produced with the goal of artificially improving (or damaging) the ratings of the product.

Hate Speech: Speech that attacks a group (or, sometimes, a person) based on categories like race, sex, religion, origin or disability. Its goal is to incite prejudice and spread bigoted views.

Misinformation: False content that is the product of error (i.e., whose originator or distributor may not be aware that the content is not truthful).

ENDNOTES

- ¹ www.mywot.co
- ² www.snopes.com
- ³ www.politifact.org
- ⁴ FactCheck.org
- ⁵ <http://credibility.stanford.edu>

Crookies: Tampering With Cookies to Defraud E-Marketing

Bede Ravindra Amarasekara

 <https://orcid.org/0000-0003-1744-716X>

Massey University, New Zealand

Anuradha Mathrani

 <https://orcid.org/0000-0002-9124-2536>

Massey University, New Zealand

Chris Scogings

Massey University, New Zealand

INTRODUCTION

E-marketers are on the constant lookout for ways to generate visitor traffic to their e-commerce sites in a cost-effective manner. Search Engine Optimised (SEO) page rankings, paid-search, keyword bidding, *cost-per-mille* display advertising (CPM) and *cost-per-click* banner advertising (CPC) are some of the different ways to attract user traffic; for a fee. With the advent of *Affiliate Marketing* (AM) businesses around the globe found a new way to generate visitor traffic at a relatively low cost, using a network of affiliates (Brear & Barnes, 2008; Norouzi, 2017). Nevertheless, increasing criminal activities on Internet has made CPM and CPC advertising models prone to large scale fraud activities, such as *click-fraud* (Edelman, 2015). In this backdrop, cost-per-acquisition (CPA) appeared as the silver bullet against AM fraud, as under CPA e-commerce sites do not pay for *clicks* or for page visits anymore. The affiliates are instead rewarded only for monetary outcomes (Hu, Shin, & Tang, 2013). Though CPA is considered the safest and most cost-efficient visitor traffic generation model for Small-to-Medium Enterprises (SME), the discovery of *cookie stuffing* fraud shows that it is not the silver bullet that it was thought to be. Though at a much lesser degree, some fraudulent activities have been recently discovered (Amarasekara, 2017; Chachra, Savage, & Voelker, 2015; Edelman & Brandi, 2015).

During this research an AM strategy of a current practitioner was examined. Two datasets of AM-generated web traffic data were analysed to detect any possible fraudulent patterns. These two datasets were separately generated by two different Affiliate Marketing Networks (AMN) that managed AM services for the same practitioner at two different periods of time. A test environment was developed, named AMNSTE (Amarasekara & Mathrani, 2016), which can simulate the complete set of processes that underlie web-traffic generation within a real-world AM network, using the same underlying technologies. AMNSTE consists of multiple virtual servers within different web domains. They are connected by virtual switches and routers that allow inter-domain routing. While AMNSTE has the ability to add new domains and additional servers, a minimum test configuration comprises of three web domains, each representing one of the three stakeholders in AM: Advertiser (e-commerce site), the AMN (tracking service provider), and at least one Affiliate website. Each of the three domains comprises a web server to host the website or web-services and a database server to save transaction and tracking data. Fraudulent

DOI: 10.4018/978-1-5225-9715-5.ch073

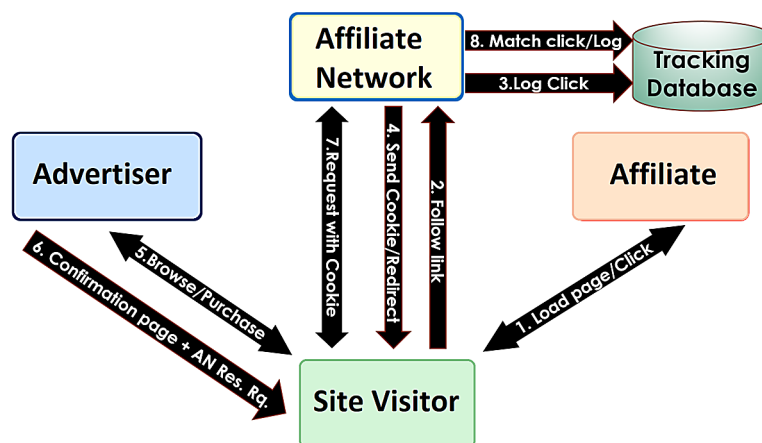
actions discovered within datasets were tested through simulations on AMNSTE, and multiple fraudulent methods were discovered to execute some of the currently known frauds. AMNSTE also allowed the authors to discover newer vulnerabilities that can be used by fraudsters in future, to defraud AM networks. The solutions proposed here were tested on AMNSTE for efficacy and utility.

This paper provides an insight in to how cybercrime is effecting e-commerce activities by endangering one of the most affordable and cost-effective traffic generation models available to SMEs. The paper first introduces the reader to the topic of Affiliate Marketing, and the underlying tracking technology based on the HTTP cookie. Then, it provides a technical perspective to the frauds that are currently known such as *Cookie stuffing* by explaining how those frauds are accomplished. It then describes new vulnerabilities that have been discovered by the authors during their current research project, which could be exploited by fraudsters in future. Next, the authors propose solutions on how to mitigate the risks, which would enable e-commerce practitioners to implement new solutions or re-examine their existing security strategies. Finally, the conclusions and future research directions are discussed that could make the tracking system more robust and reliable, in order to sustain this cost-efficient and affordable marketing model.

BACKGROUND

Affiliates are independent websites who already have a large following of visitor traffic, who might belong to the potential target market of some product advertisers. Affiliate marketing model uses a network of such affiliates, who will promote the advertiser's website, usually by displaying a banner advertisement. Figure 1 provides a logical view of the AM process, starting from a visitor's click on a banner advertisement at an affiliate's website to the completion of a purchase action. The sequence of the processes involved are numbered in the diagram. When a user views an affiliate website (process 1) and clicks an advertisement link (process 2) the "Click Pixel" embedded in the webpage causes the tracking server to create a record of the "click" action in the database (process 3). The tracking server then sends a cookie to the browser with a unique identifier that refers to this specific click. It also sends a redirect response to the browser, targeted at the advertiser's e-commerce site (process 4). The visitor then browses the e-commerce site and makes a purchase decision (process 5). The process 6 is abbreviated as "AN Res. Rq.", which stands for "Affiliate Marketing Network resource request", which refers to the "Conversion Pixel" embedded in the payment confirmation page sent by the e-commerce serve. In the background without any visible clue to the user the *Conversion Pixel* causes the user's browser to send a resource request to the tracking server with the information such as the Invoice Identifier, total purchase price, etc. as parameters of the resource request. As every HTTP request to the web server is accompanied by the cookies that the server has set previously, in this case during the click-tracking process numbered 3, the tracking server records the sales conversion details against the click-tracking data in the database. The *Click Pixel* and *Conversion Pixel* are small pieces of JavaScript code that are embedded in those webpages that provide user-specific information to the tracking server. The tracking server, while being invisible to the user, keeps track of all processes and traffic movements with the help of *tracking-cookies*. Next, how the above cross-domain tracking systems are used by different marketing models are discussed.

Figure 1. Logical view of an affiliate marketing process



Affiliate-Driven E-Marketing Strategies

Different advertising models yield different levels of visitor interactions and commitments, therefore different levels of Return on Investment (ROI) for the e-marketers. For example, CPM and *paid search* models do not guarantee any *visitors* to the e-commerce site as affiliates are paid simply for displaying the advertisement to the site-visitor; the visitor might neither click the advertisement nor even see the advertisement. Only about 1% of site visitors actually go on to click on a banner advertisement (Benediktova & Nevosad, 2008). But CPC model requires more visitor interaction, as an affiliate earns a fee only if the visitor in fact clicks on the advertisement and thereby arrives at the e-commerce site. Though there is no guarantee that a visitor may buy a product, the affiliate is nevertheless paid a fee, for the visitor-traffic. In contrary, CPA model is becoming increasingly popular among e-marketers, as affiliates are only paid for successful monetary outcomes, not for clicks or displays, thus guaranteeing ROI for the e-marketer. Therefore, the cost of each advertising model differs greatly from mere tenth of a cent for display advertising, to 5-10% of the sale value as a commission in case of CPA (Faou, et al., 2016).

Advertisers can either monitor and manage their own network of affiliates by themselves or subscribe to a third-party AMN.

HTTP-Cookies Driving the Tracking Technology

HTTP cookies have been used to maintain state in web applications that are inherently stateless. Though maintaining state during browsing sessions and during subsequent visits to the same websites enhances the user-experience, tracking user activities that does not directly contribute to the enrichment of user experiences is much frowned upon by most users (Hoofnagle, Urban, & Li, 2012). User activity on the internet is tracked for many reasons and by different parties: Some reasons for tracking are directly beneficial to the internet user, such as remembering user-preferences such as language, currency, shopping cart items, login etc., while some other reasons are for the benefit of the web-sites and e-commerce sites to gather additional customer demographics. Such additional visitor specific information help enterprises with their targeted marketing strategies. E-commerce sites also track locations of users and IP addresses during transactions for enhanced security but they also add to customer demographics used for business

analytics purposes. The above reasons for tracking directly relate to the interaction between a website and a visitor to that site, and is limited to tracking a user within a single web domain.

Some services and their underlying technologies that are used widely in e-commerce activities on the internet such as AMNs and other performance marketing models require a reliable tracking technology across multiple domains, in an inherently stateless ecosystem. This type of tracking is a technological necessity, invisible to the visitor and the website, and is not detrimental to the privacy of users, as no personally identifiable data is used in such scenarios. HTTP cookies have been used for such cross-domain tracking (Kristol, 2001), though newer technologies such as *local storage* offered by HTML5 and *ETags* could enhance the reliability of the HTTP cookie based tracking process (Ayenson, Wambach, Soltani, Good, & Hoofnagle, 2011; Soltani, Canty, Mayo, Thomas, & Hoofnagle, 2010).

But search engines and business analytic solution providers such as Google Analytics need to track activity over multiple sites and over longer periods. User-activity tracking data contained in HTTP cookies are combined with personally identifiable data collected through user accounts maintained by the above service providers and social media accounts to create comprehensive customer profiles that are used for online marketing strategies (Baumann, Haupt, Gebert, & Lessmann, 2018). Recent privacy breaches involving Cambridge Analytica (Richterich, 2018) and Facebook are examples of more serious violations of privacy of Internet users. Apart from that, user-tracking is also undertaken by state agencies, departments and other law enforcement agencies to monitor terrorist activities and to counter spy-activities to maintain national security. This category of user-tracking is beyond the scope of this chapter and is not discussed here.

HTTP Cookies have *properties* associated with them. These properties are set by the web server, when the cookie is created, and those properties decide the behaviour of the cookie. *Secure* property ensures that the cookies are sent only on an encrypted HTTPS connection, while *HTTPOnly* property makes a cookie content only accessible to the server but not to the JavaScript code on the browser. Another important property is *Expires* property that determines the lifespan of the cookie. *Domain* and *path* properties restrict if the cookie is sent with requests of the sub domains and resources from specific file paths. The browser returns the cookie only to the hosts of the same domain that set the cookie (HTTP cookies, 2018). If the cookie belongs to the same domain as the web page, such cookies are called *first-party* cookies. If the cookie belongs to a different domain than the web page, then it is a *third-party* cookie. Third-party cookies are usually placed by business analytics services or advertising service providers (Eckersley, 2010; Hoofnagle, Urban, & Li, 2012). Though a web page would usually contain links to resources that reside within the same domain and same server, third-party web advertising companies and business analytic service providers might include a resource such as an image to be delivered from their servers, so that a cookie from their domain can give access to the user's browsing behaviour (Libert, 2015). Browsers by default allow third-party cookies to be received, but it can be a security risk (Kristol, 2001).

Click-Tracking vs. Conversion-Tracking

Click-advertising or display-advertising models such as CPC or CPM are traffic generation models that pay affiliates agreed sums of money for displaying advertisements or when a visitor clicks on an advertisement, immaterial of a successful monetary outcome such as a sale. Therefore above advertising methods do not need to track ongoing interactions of visitors with e-commerce site. The initial action of displaying or clicking is recorded on a tracking server.

Under performance advertising model such as CPA, where only monetary outcomes yield a benefit to the affiliate, the tracking process comprises of two separate actions. The click-tracking records the click action first. A *conversion-pixel* embedded in the payment confirmation page of the e-commerce site, causes the visitor's browser to initiate a conversion-tracking action. After recording each conversion, the conversion tracking process looks up the click-tracking database for a corresponding *click-record*, with the same affiliate identifier and advertiser identifier.

A conversion tracking action without an accompanying tracking-cookie (when HTTP cookies are used for tracking) or without valid affiliate identifier are considered as direct sales, which are a result of the customer having come to e-commerce site directly by typing the URL in to the browser, or through organic search. In this case no affiliate payments are made, as no affiliate has been involved in that sale.

Click-Pixel and Conversion-Pixel

As a small piece of HTML or JavaScript code *click-pixels* are embedded in the web pages of affiliates, usually as a URL of an embedded banner advertisement. Some affiliates use such a click-pixel on e-mails sent to customers. Each affiliate is provided with a unique click-pixel that contains a URL to the tracking server with a unique identifier for each affiliate, passed as a parameter. A click-pixel causes the tracking server to record a click-tracking action identifying the affiliate and places a HTTP cookie in the user's browser. Click-pixels are usually implemented as a graphic image of a banner advertisement or as a hyperlink in a text advertisement.

A Conversion-pixel is embedded as an HTTP image element or invisibly as an HTML iframe element on the payment confirmation page. This causes each successful purchase by an e-commerce site visitor to be recorded on the tracking database. The tracking URL of the conversion-pixel can contain information such as the total price, transaction identifier, etc., and the HTTP cookie that was placed during the click-tracking process on the user's browser will identify the affiliate who promoted the visit.

Pixels can be embedded in any webpage that need to be tracked with specific outcomes, by passing relevant information that need to be tracked as parameters of the tracking URL. Usually a combination of an HTML based and a JavaScript based pixel is used, as JavaScript based pixel can use powerful client-side scripting capabilities to offer additional robustness to the tracking process.

CLICK FRAUDS AND CONVERSION FRAUDS

Edelman and Brandi (2015) have discussed some fraud scenarios such as cookie stuffing and typo-squatting. Chachra et al. (2015) and Snyder and Kanich (2016) have quantified the fraud prevalence within AM. The litigation against Shawn Hogan by e-bay in 2013 for AM fraud of over 15 million US dollars indicate the volume of some AM fraud (Edelman, 2015).

What Amounts to a Fraud Action?

Advertisers expect affiliates to be active participants in the process of promoting and influencing a visitor's decision to visit one or more e-commerce sites of advertisers, for which affiliates are paid a fee or a commission. Usually this happens by displaying banner advertisements on affiliates' websites and causing or motivating the visitors to click them to arrive at the e-commerce site. Any attempt to claim

the fee or commission, without participating or contributing to the decision or motivation of a visitor to the e-commerce site of an advertiser is therefore a fraud.

These frauds depend on the ability of a rogue affiliate to insert a click- or conversion-record in to the tracking database. This can be undertaken in two different ways:

1. By following and adhering to the intended underlying technology

Fraudulent action within this category, do not manipulate tracking records in the server or the technical aspects of the tracking process itself, directly. It is involved in simulating a *click* action of a visitor on an advertisement banner, manually or programmatically, and letting the natural cause of actions and underlying technology to complete the process of the fraud activity.

2. By foregoing the tracking process and manipulating the tracking data on server

This does not refer to usual server-hacking activity, as a hacker who gains access to a server in an illegitimate manner can cause multitude of damaging activities that are not discussed in this chapter. The verity of activities discussed under method refers to accessing the tracking server's publicly exposed service URLs by external parties or internally accessible interfaces by internal staff to manipulate tracking data. The externally accessible public URLs are meant for the interaction with automated tracking process, while internal access is meant for maintenance activities for the internal staff.

How this can be accomplished is discussed further below under each fraud description.

Cookie Stuffing

Cookie stuffing is the most widely known HTTP cookie-based tracking fraud that has been mentioned in previous research studies. As affiliate websites are usually special interest websites which are popular among specific interest groups, and usually have a large following, too many advertisements can affect the credibility and seriousness of such websites. A rogue affiliate can maintain a website free of advertisements, thus appear serious and credible, while causing the browser of each visitor to receive tracking-cookies from one or more advertisers, through an automated process of simulating *clicks* even when the visitor has not clicked on any advertisement banner. Each of these cookies will earn the rogue affiliate a commission, if the visitor makes any commercial transactions at any of those e-commerce sites. The visitor will be completely unaware of the background processes and receiving of cookies.

Using AMNSTE, it was possible to execute this fraud in multiple different ways. HTML code that requests a resource from the server, such as an image, icon, JavaScript or CSS file, where the source property is set to a tracking URL of a server causes the tracking server to record a *click* in its database and send a cookie containing the affiliate's identifier to the browser. The same result was also accomplished by using a CSS file, where for instance, the background image was defined by CSS code, with the image URL set to a tracking server URL. A rogue affiliate can maximise his profits by embedding numerous such elements, where each element is directed at a different tracking URL, thus stuffing cookies of many different advertisers. This caused the browser to send resource requests to each of the tracking servers, while the affiliate's web page is loaded, and in return the browser received cookies containing the rogue affiliate's identifier from each of those advertisers, denoting that the request originated from affiliate's website. Any future purchases made by the unsuspecting visitor at any of those advertisers' e-commerce sites would earn a commission for the affiliate.

This type of cookie stuffing can earn large profits for a rogue affiliate in some instances. For example, if the affiliate site is a travel blog about travelling around in New Zealand, it is highly likely that many visitors to the travel blog site might be planning a visit to New Zealand at some point in time, in future. The affiliate would stuff as many cookies from each hotel chain, car rental companies, airlines and tourism related service providers, as it is likely that the visitor to the affiliate's travel blog might visit some of those e-commerce sites to book a product or service. At such time, the previously stuffed cookie will identify the rogue affiliate as the referrer. This allows a rogue affiliate to cash in large amounts of commission money from multiple advertisers by using one site visitor.

Load-Time Click

This fraud is similar to cookie stuffing, but instead of static HTML or CSS code this fraud uses JavaScript code to dynamically simulate *click* actions of a user. An affiliate can present a webpage free of any third-party advertisements to the visitor, but without visitor's intervention simulate *click* actions on as many advertisements at will during the load event of the webpage. This fraud differs from cookie stuffing as Cross Origin Resource Sharing (CORS) restriction restricts browsers from accepting HTTP cookies in response to JavaScript code, hence can be used for CPC to emulate multiple banner clicks. But, the above restriction is only a client-side implementation, therefore the client computer still receives the cookie, which might still pose a threat similar to cookie-stuffing.

Conversion Stealing

The authors found conversion stealing to be the most serious fraud that affect advertiser revenue, in a previous study (Amarasekara & Mathrani, 2016). This fraud can be carried out as an internally or externally executed fraud, with internally executed fraud being the most damaging to the advertisers. The methods and complexity differ with internal and external threats. The aim of this fraud is to recognise the transactions that are direct sales, and attribute them to a rogue affiliate within the tracking database. This fraud affects mainly performance marketing models such as CPA, which depend on successful monetary outcomes unlike CPM or CPA models that are only concerned with display or click actions, not purchase outcomes. When executed as an internal fraud, a fraudster can create an automated process that queries the transaction database for direct sales and choose as many of them depending on applied criteria, such as specific number of highest valued transactions (or all, if one is too greedy) and insert new tracking records with those information in to the tracking database. New tracking records can be inserted using Web Application Programming Interfaces (WebAPI) provided by AM Networks for manual maintenance and update purposes or the fraudster can use externally accessible conversion-tracking web services URL. Such fraudulent records can evade detection even in case of many reconcile applications, as the newly inserted tracking records do refer to actual existing transactions, for which no commissions have been previously paid to any affiliate. Even a contract web developer without ongoing access rights to an internal system can implement this kind of an automated process during a one-time assignment that earns a regular monthly commission income for many years to come.

An external fraudster will need to find data parameters often through brute force or with trial and error guess work. Creating a single genuine transaction by the fraudster will reveal a transaction identifier that gives the clue to genuine transactions identifiers that can be used for forgery, as many systems generate transaction identifiers in sequence.

Conversion stealing does not have to happen in real-time with each conversion, but an automated process can do the data mining on transaction databases and assign selected transactions to the rogue affiliate, before the next payment cycle.

Conversion Faking

This fraud is another variation of conversion stealing, but in contrary, does not attempt to insert authentic transaction data in to the tracking database. Therefore, this fraud does not require the fraudster to have application-level access rights to the system or use an automated process within AM Network to insert the conversion records to the tracking database as conversion stealing does. This fraud can be carried out by any rogue affiliate. The success of this fraud depends largely on the security precautions implemented by the AM practitioner. If an AM practitioner depends completely on the security framework of the AM network to prevent fraud, and to filter and eliminate all fraudulent records, without implementing a transaction reconcile process on the AM practitioner's side, *conversion faking* can be highly successful for the fraudsters. In such case, a fraudster would guess transaction identifiers or invoice totals and use these information as URL parameters of the conversion-pixel, which can be found by examining the HTML/JavaScript code on confirmation page, after one successful transaction. This fraud can also be carried out programmatically, or typing the URL of the *conversion pixel* together with the required parameters manually in to a browser's URL field or embedding a hyperlink on a webpage under the control of the rogue affiliate.

Conversion Hijacking

This is a similar fraud that happens in real-time as the transaction. This is carried out externally unlike *conversion stealing*, as this fraud does not need access to the transaction databases. Adware, malicious browser plugins or similar malicious software that has infected a visitor's computer can sniff online activity, and trigger the corresponding *click-pixel* code just before the purchase (Edelman & Brandi, 2015). This will cause a cookie to be placed in the visitor's computer and the commission to be assigned to the rogue affiliate identified in the cookie.

Multiple Redirect Fraud

The *Referrer* field of the HTTP request headers reveal the last visited webpage of a visitor. Rogue affiliates cover their footprints by using multiple redirects over websites that contain legitimate content to conceal the origins of fraudulently generated web traffic (Chachra, Savage, & Voelker, 2015; Snyder & Kanich, 2016; Vacha, Saikat, & Yin, 2013). This can be used in conjunction with the other frauds mentioned above to make detection of frauds more difficult.

Typo-Squatting

Some of the frauds such as typo-squatting and keyword-bidding are considered a fraud by some advertisers, while others consider it legitimate. This depends on the advertiser's contractual agreements and different e-marketing strategies they may have used. Typo-squatting is when an affiliate acquires domain names that are very similar to an advertiser's domain (Edelman & Brandi, 2015). By squatting on similar sounding fake URLs, the affiliate captures the traffic of visitors who either mistypes the advertisers

name or types a confusingly similar name. After capturing the visitor, the affiliate can either redirect to the intended advertiser with a cookie to identify the affiliate and thereby earning the commission or forward to a website of a competitor for higher reward.

However, other non-technology based frauds too can incur heavy losses by using simple deceitful actions like temporarily occupying bookings. On most e-commerce sites, for example at a hotel or a car rental company affiliates can themselves book a car or a room a few months in advance and earn a hefty commission before eventually cancelling their booking after a few months. The rogue affiliate squats on bookings which they have no intention of honouring. Since many advertisers pay the commission at the end of the month following the purchase, the undeserving affiliate would be paid a commission not rightfully earned.

Non-Technology Based Fraud

Even non-tech savvy rogue affiliates can still inflict financial losses through conventional fraud methods that are used in other scenarios. For example, most reservation sites allow goods or services to be reserved many months in advance. Rogue affiliates can make an authentic reservation few months ahead of time, by themselves and thereby earn a hefty commission, and cancel the reservation later. Under CPC and CPM marketing models, *click-factories* of manual clicking of advertisements and using proxy servers to hide IP addresses of origin have been widely discussed in previous research. Credit card fraud such as using stolen credit cards to make reservations also fall under non-technology based frauds that are not covered in this paper.

MANAGING FRAUDS AND VULNERABILITIES

There is no one single action that can eliminate all the frauds discussed above, as frauds are numerous and the way they are executed are accordingly numerous. The different actions that we discuss below can be combined to create an effective solution to combat fraud scenarios. All conversion records, that do not have an accompanying tracking cookie indicate direct customers, an organic search traffic or a visitor traffic generated through non-AM method. Therefore no commissions are paid on behalf of those sales, and they need to be filtered out.

AM practitioners who have an in-house implementation of AM strategy, can implement the solutions proposed in this paper, as they manage the tracking data as well as e-commerce transaction data. AMNs who provide technology for AM practitioners are entrusted to detect and filter out all fraudulently generated visitor traffic and to provide the AM practitioners with an authentic set of records with legitimate traffic generation data, ready for commission payment. Some of the most important techniques that are presented in this chapter, require access to e-commerce transaction data which are not available to the AMN.

Reconcile Records

The next single most important step, is to reconcile *conversion-tracking* data with the backend transactional database of online sales. In an in-house tracking network, both tracking database and online sales transaction database are located within the private internal network, therefore a reconcile process can be integrated between tracking database and online sales transaction database. In a third-party AMN

tracking scenario, most AMNs provide Web API access to the tracking databases located in the AMN network. Web API access allow direct communication between servers, even when they are located in different domains, to securely connect and undertake CRUD (Create, Read, Update & Delete) activity. During reconcile process, the transaction identifier, transaction amount and date & time field of each conversion record should match a single online sales transaction in the transaction database. The first *filtering* process is rather easy and straightforward as it separates conversions forged by fraudsters with imaginary transaction IDs and total prices, that have been guessed. Next few steps can further filter out fraud action, and these can be carried out in a specific order, that would yield maximum benefit, depending on the setup of individual systems.

Check “Referrer” Field

Conversion pixel is placed in the payment confirmation page of the e-commerce site. Therefore, any conversion record that carries a different page URL or an empty *referrer* field, is a fraud, that has to be filtered out. Similarly, *click pixel* is placed in affiliate’s landing page. Advertisers need to maintain a record of all the pre-authorised landing page URLs of the affiliates. Click records with *referrer* fields that are either empty or contain unauthorised URLs should be rejected.

Audit Manual Entries in Tracking Database

Web API access provided by AMNs, discussed above is used to update specific fields of tracking records during the reconcile process; ex: toggle the *pending* status to *reconciled* or *paid* or *cancelled* statuses. Usually, new entries should not be added manually, as adding click- or conversion-tracking entries happen automatically, through the tracking process, using click- and conversion-pixels embedded in the web pages. *Conversion stealing* usually does not happen in *real-time*, hence, two different processes can be undertaken to detect this fraud.

Firstly, checking for addition of new tracking records using Web APIs should be audited, which are tell-tale signs of such tampering. Secondly, an automated process should compare the timestamp of each *conversion tracking* entry with the timestamp of the actual transaction. A large time difference points at a possible *conversion stealing*.

Crawl Affiliate Landing Pages

As part of regular maintenance activity, an automated process can be scheduled to crawl each authorised landing page of each affiliate. If the crawler receives any cookies during the crawl process, it indicates *cookie stuffing* fraud, as the crawler does not trigger any click actions. Some tech-savvy fraudsters are known to have implemented code in their landing pages, to recognise such crawlers and serve a *clean page* instead of the usual fraudulent page, thereby evading detection (Chachra, 2015). We need to be a step ahead of such fraudsters by concealing the identity of the crawler, by dynamically changing the *user-agent* and *referrer* fields of the HTTP request and hiding IP address using proxy servers and VPNs, etc.

Use of Buffer Tables

All online transaction data should be directed to a *buffer* table in the database, without exposing the internal transaction-related tables. For example, reservation data is entered in to *Reservation Buffer* table, assigning a unique reservation identifier, and the same record is mapped to an entry in the internal *Reservation Table* with a different reservation identifier. Within the complete internal system, the specific reservation record will be linked to the internal identifier in the *Reservation Table* while all actors external to the system, such as customers, front-line staff etc. refer to the specific reservation record with the Identifier generated by reservation buffer table. Same can be done using a *Payment Buffer* table and an internal *Payment Table*. Our research recognised attempts by external parties and in once occasion, by an internal staff of the advertiser who entered forged *conversion* records to the tracking database, but using the reservation identifier allocated by the *Reservation Buffer* table. During the reconcile process, such *conversion* entries get rejected, as the records get reconciled against the internal reservation identifier.

Audit Visitor Logs

Web server log or custom developed visitor logging features can reveal some irregular patterns that point at possible fraud attempts. For example, the web based reservation system of the AM practitioner that was examined by the authors had the facility for a customer to recall an active reservation made by the customer by entering the transaction code. This allowed the customer to view and modify a reservation. Our audit of webserver logs of the AM practitioner revealed regular brute-force attacks to extract authentic transaction identifiers from the system. Large number of repeated attempts, from the same IP address, within milliseconds apart pointed at automated processes, while some within a few dozens of seconds pointed at possible manual brute-force attacks.

FUTURE RESEARCH DIRECTIONS

As with every other IT security effort, researchers need to stay ahead of the attackers and fraudsters who also continue to refine their tactics to evade detection. Ongoing research activities of the authors are directed at hardening and making the HTTP cookie based tracking system more robust by complimenting HTTP cookie based tracking technologies with client-side technologies such as *HTML5 Local storage*, *ETags*, etc. (Laperdrix, Rudametkin, & Baudry, 2016; Snyder, Ansari, Taylor, & Kanich, 2016). The effectiveness of using a mix of stateful and stateless tracking methods need to be investigated (Englehardt & Narayanan, 2016).

The software industry has an opportunity to invest in research and development of standardised solutions to cater to the e-marketing platforms that would result in continuous and timely application of security measures to counter evolving vulnerabilities.

CONCLUSION

Access to the internet is expanding throughout the globe and more people spend more time connected through multitude of devices, for daily needs. Products are purchased and services are subscribed to, beyond physical and geographical boundaries that allows even small entrepreneurs in developing

countries and developed countries alike, to reach customers across the globe. CPA method of affiliate marketing model allows SMEs to reach the target markets without the technical expertise required for many other forms of e-marketing technologies. It also shifts the marketing paradigm of the need to spend an advertising budget before reaching out to potential customers; under CPA advertising cost for traffic generation is paid by profits of the sale (Norouzi, 2017). Therefore, the survival and development of this cost-efficient technology depends on continuous research and development of solutions to mitigate fraud and vulnerabilities, and implementation thereof by the industry.

REFERENCES

- Amarasekara, B. R. (2017). *Analysis, design and simulation of fraud and vulnerability management in affiliate marketing: a thesis submitted to the Massey University of Auckland in fulfilment of the requirements for the degree of Master of Philosophy, Massey University of Auckland*. Auckland, New Zealand: Massey University. Retrieved from <http://hdl.handle.net/10179/12128>
- Amarasekara, B. R., & Mathrani, A. (2016). *Controlling Risks and Fraud in Affiliate Marketing: A Simulation and Testing Environment*. PST2016 (Privacy, Security and Trust - IEEE 14th Annual Conference), Auckland, New Zealand.
- Ayenson, M., Wambach, D., Soltani, A., Good, N., & Hoofnagle, C. (2011). *Flash Cookies And Privacy II: Now with HTML5 and ETag Respawning*. World Wide Web Internet and Web Information Systems.
- Baumann, A., Haupt, J., Gebert, F., & Lessmann, S. (2018). The Price of Privacy: An Evaluation of the Economic Value of Collecting Clickstream Data. *Business & Information Systems Engineering*, 1-19. doi:10.1007/12599-018-0528-2
- Benediktova, B., & Nevosad, L. (2008). *Affiliate Marketing - Perspective of content providers*. Department of Business Administration and Social Sciences. Lulea University of Technology.
- Brear, D., & Barnes, S. J. (2008). Assessing the value of online affiliate marketing in the UK financial services industry. *International Journal of Electronic Finance*. doi:10.1504/IJEF.2008.016881
- Chachra, N. (2015). *Understanding URL Abuse for Profit*. San Diego, CA: University of California.
- Chachra, N., McCoy, D., Savage, S., & Voelker, J. M. (2014). Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting. *Proceedings of the Workshop on the Economics of Information Security (WEIS)*. Retrieved from <https://cseweb.ucsd.edu/~voelker/pubs/namevalue-weis14.pdf>
- Chachra, N., Savage, S., & Voelker, G. (2015). Affiliate Crookies: Characterizing Affiliate Marketing Abuse. In *IMC '15 Proceedings of the 2015 ACM Conference on Internet Measurement Conference* (pp. 41-47). New York, NY: ACM. doi:10.1145/2815675.2815720
- Eckersley, P. (2010). *How unique is your web browser? Privacy Enhancing Technologies*. Springer.
- Edelman, B. (2015). Retrieved from Affiliate fraud litigation index: [http:// www.benedelman.org/affiliate-litigation](http://www.benedelman.org/affiliate-litigation)
- Edelman, B., & Brandi, W. (2015, February). Risk, Information, and Incentives in Online Affiliate Marketing. *JMR, Journal of Marketing Research*, 52(1), 1–12. doi:10.1509/jmr.13.0472

- Englehardt, S., & Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery. 10.1145/2976749.2978313
- Faou, M., Lemay, A., Deary-Hetu, D., Calvet, J., Labreche, F., Jean, M., ... Fernandez, J. M. (2016). Follow the traffic: Stopping click fraud by disrupting the value chain. In *14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE. 10.1109/PST.2016.7907001
- Hoofnagle, C., Urban, J., & Li, S. (2012). Privacy and Modern Advertising: Most US Internet Users Want ‘Do Not Track’ to Stop Collection of Data about their Online Activities. *Amsterdam Privacy Conference. HTTP cookies*. Retrieved from Mozilla Developer Network: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>
- Hu, Y., Shin, J., & Tang, Z. (2013). *Performance-based Pricing Models in Online Advertising: Cost per Click versus Cost per Action*. Atlanta, GA: Georgia Institute.
- Kristol, D. M. (2001). HTTP Cookies: Standards, Privacy, and Politics. *ACM Transactions on Internet Technology*, 1(2), 151–198. doi:10.1145/502152.502153
- Laperdrix, P., Rudametkin, W., & Baudry, B. (2016). Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints. 37th IEEE Symposium on Security and Privacy (S&P 2016).
- Libert, T. (2015). Exposing the Invisible Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites. *International Journal of Communication*.
- Norouzi, A. (2017). An Integrated survey in Affiliate Marketing Network. *Press Academia Procedia*, 42, 299–309. doi:10.17261/Pressacademia.2017.604
- Snyder, P., Ansari, L., Taylor, C., & Kanich, C. (2016). Browser Feature Usage on the Modern Web. In *Proceedings of the 2016 Internet Measurement Conference (IMC '16)* (pp. 97-110). Santa Monica, CA: ACM. 10.1145/2987443.2987466
- Snyder, P., & Kanich, C. (2016). Characterizing fraud and its ramifications in affiliate marketing networks. *Journal of Cybersecurity*, 2(1), 71–81. doi:10.1093/cybsec/tyw006
- Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. (2010). Flash Cookies and Privacy. In *AAAI Spring Symposium: Intelligent Information Privacy Management*, (pp. 158-163). AAAI.
- Vacha, D., Saikat, G., & Yin, Z. (2013). ViceROI: Catching Click-Spam in Search Ad Networks. In *ACM Conference on Computer and Communications Security* (pp. 765-776). New York, NY: ACM. doi:10.1145/2508859.2516688

ADDITIONAL READING

Amarasekara, B. R., & Mathrani, A. (2017). Revenue fraud in e-commerce platforms: Challenges and solutions for affiliate marketing. In A. Colarik, J. Jang-Jaccard, & A. Mathrani (Eds.), *Cyber security and policy: a substantive dialogue* (pp. 67–87). Auckland, New Zealand: Massey University Press.

Edelman, B. (2014). Mastering the intermediaries: Strategies for Dealing with the Likes of Google, Amazon, and Kayak. *Harvard Business Review*, 92(6), 86–92. PMID:25051857

Fox, P., & Wareham, J. (2007). Controlling your brand: Contractual restrictions placed by Internet retailers on affiliate marketing activities in Spain. *BLED 2007 Proceedings*.

Kayalvizhi, R., Khattar, K., & Mishra, P. (2018). A Survey on Online Click Fraud Execution and Analysis. *International Journal of Applied Engineering Research*, 13, 13812–13816.

Krishnamurthy, B., & Wills, C. E. (2009). Privacy diffusion on the web: A longitudinal perspective. *WWW'09-18th International World Wide Web Conference*, (pp. 541–550). Madrid, Spain. doi:10.1145/1526709.1526782

Libai, B., Biyalogorsky, E., & Gerstner, E. (2003, May). Setting Referral Fees in Affiliate Marketing. *Journal of Service Research*, 5(4), 303–315. doi:10.1177/1094670503005004003

Mathur, A., Narayanan, A., & Chetty, M. (2018). Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest. *Proceedings of the ACM on Human Computer Interaction*, 2. New York, NY. 10.1145/3274388

Miehling, M., Buchanan, W. J., Old, J., Batey, A., & Rahman, A. (2010). Analysis of Malicious Affiliate Network Activity as a Test Case for an Investigatory Framework. *9th European Conference on Information Warfare and Security*.

Official Journal of the European Union. (2016). General Data Protection Regulation. Retrieved from <http://data.europa.eu/eli/reg/2016/679/oj>

Richterich, A. (2018). How Data-driven research fuelled the Cambridge Analytica controversy. *The Open Journal of Sociopolitical Studies*, 11(2), 528–543. doi:10.1285/i20356609v11i2p528

KEY TERMS AND DEFINITIONS

AMNSTE: An acronym for a research tool developed by the authors during the on-going research project, Affiliate Marketing Network Simulation and Testing Environment, which has been previously published.

Conversion: A visitor to an e-commerce site completes a desired monetary transaction such as buying product or signing up for a service or a membership or whatever expectations an e-commerce site is intended to achieve by having visitors to the e-commerce site. A visit converts to a monetary outcome.

CPA: Cost-per-acquisition advertising model pays affiliates only for visitor traffic that generated an income for the e-commerce site.

CPC: Cost-per-click advertising model pays affiliates for each visitor that was re-directed to the advertiser's e-commerce site, immaterial of the financial outcome; even if the visitor does not buy any products.

CPM: Cost-per-mille advertising model pays affiliates for simply displaying an advertisement of the e-commerce site to a visitor to the affiliate's website. This model requires least interaction by a visitor.

ETag: Entity Tag is a server-side identifier assigned to content for cache-control. The browser caches and sends the ETag on subsequent web requests, which allows the server to send the resource only if the server version has changed. ETag can also be used to track users uniquely, online.

HTML5: Version 5 of hypertext mark-up language which was released in October 2014 added major improvements and features such as ability to handle multimedia and graphic features natively, and a web storage framework that can store data similar to previous usage of cookies.

HTTP Cookie: Due to security reasons, websites visited by an Internet user are not allowed to access the internal storage of the visitor's computer, such as the hard disk. The only way to store a small amount of data such as visitor's preferences, which is individual to each visitor is to store it within the browser's storage, as plain text. Such storage is called a cookie, which was in earlier browsers a text-based file on the visitor's computer. But now each browser decide how it stores. Though a browser may have many hundreds of cookies, each saved by a different website, each website can only access the cookie that it has placed, but not the cookies placed by another website.

Stateful Tracking: Using identifiable information stored in a user's local computer, such as an HTTP cookie to identify a visitor's computer uniquely on the internet.

Stateless Tracking: Does not store any identifiable information on a user's computer. A combination of unique signatures about each computer is stored in the tracking server, which can identify a computer with a relative high accuracy, but not as precisely as stateful tracking methods.

Crime Identification Using Traffic Analysis of HTTP Botnet

Ciza Thomas

 <https://orcid.org/0000-0002-1030-3000>

Directorate of Technical Education, India

INTRODUCTION

A botnet is a network of malware infected systems that are controlled by an attacker through a Command and Control (C&C) channel. The attacker, also called the botmaster, controls the infected systems that are called bots or zombies. Various types of cyber-crimes are done by the botmaster with the help of these bots. A group of bots under the control of a botmaster is called a botnet. The general layout of a botnet system is shown in figure 1. The attackers use botnets to create disruption on the network or on a victim host either by utilizing the entire bandwidth in that network with bogus connections or by 100% CPU utilization on the victim host. This is through commanding the compromised bots to overload the resources of the victim machine/ network, to the point that it stops functioning resulting in denial of access. Such an attack is called a denial of service (DoS). Botnets can be used by botmaster to perform distributed denial-of-service (DDoS) attack, steal data, send spam, and access the device and its connection. These cyber-crimes are constantly evolving and hence the list of cyber threats can at no stage be considered exhaustive. Thus botnets are a great threat on the Internet by serving as the basic infrastructure for various distributed attacks.

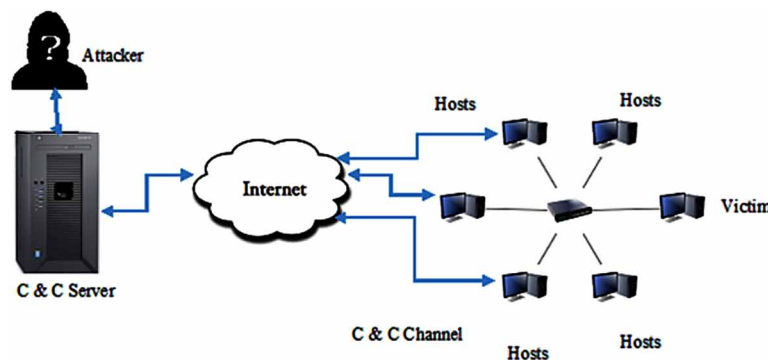
Botmasters can use HTTP protocol for the C&C channel as majority of the Internet traffic uses HTTP and hence are allowed in most of the networks. Effectively, bots hide their communication within the normal HTTP traffic as it is not easy to block this service as a precautionary measure. This fact makes the HTTP-based C&C communication stealthier. Centralised C&C channels are prone to single point of failure as the C&C channel if detected and stopped, results in the loss of the communication channel between the compromised hosts. The advantage of centralised C&C channels is that they are simple and easy to setup as highlighted in Gu and Perdisci (2008). Botmasters have moved to peer-to-peer (P2P) C&C architecture to make their bots more powerful and stealthy.

Bots run automated programs that are designed to execute specific scheduled activities or to respond to commands in a particular manner. Hence, it is expected that the botnet generated traffic should always be having an apparent structure and regularity in the behavioral pattern. This is because the normal user behaviour is totally unpredictable, random and complex. This is attributed to the innumerable online applications and resources available for users. Hence the normal traffic differs from the botnet communication traffic, which is systematic and consistent in behaviour.

Several detection strategies have been developed in the available literature for botnet detection like up-to-date anti-virus software, signature-based intrusion detection systems for IRC/botnet traffic and traffic flow monitoring for known C&Cs. These detection techniques differ based on the C&C mechanism being centralised architecture (IRC, HTTP) or peer to peer (P2P) architecture or hybrid P2P/Centralised architecture. Detection also varies depending on other factors such as area of deployment, data captured for the detection system, etc.

DOI: 10.4018/978-1-5225-9715-5.ch074

Figure 1. Typical botnet system



This work proposes a technique to collect and analyse HTTP botnets. The deficiency of publicly available botnet datasets creates the characterization of botnet traffic difficult. Hence, HTTP botnet analysis plays a key role in the design of an effective detection system due to the fact that the foremost task in the process of mitigation of a threat is its characterisation. The network traffic generated by the HTTP botnets is analysed based on various features which could be used to develop an effective detection model. In this work a framework was developed in order to build HTTP botnets in a controlled environment. Analysis of the botnet traffic shows that periodicity is a main feature of HTTP botnets. This is because of the HTTP bots periodically contact the botmaster for commands and control messages by connecting to particular URLs or web pages. In addition the bots also report their status and attack results to the botmaster. This can be utilised to build behavioural detection models at network layer as reported in the work of AsSadhan et al. (2009). Signatures of the bots that were set up are also obtained, which can be used in signature-based detection. Further analysis was done using machine learning based classification as well as periodicity analysis. The results demonstrate the superior detection performance with 100% accuracy and detection of the proposed method using the hybrid periodicity analysis.

The rest of this paper is organized as follows: The state-of-the-art of botnet structures and its detection approaches are discussed in the next section. The system architecture is subsequently discussed followed by solutions and recommendations. The paper concludes after identifying the future directions of research.

BACKGROUND

A botnet is usually established by a botnet writer developing a program, called a bot or agent, and installing the program on compromised computers on the Internet using various techniques as demonstrated by Yu et al. (2015). As botnet has now become one of the major threats in the present attack landscape, many researchers are rigorously exploring the detection, mitigation and prevention of botnets. Available literature provides details of previous research work that are carried out aimed at distinguishing or detecting HTTP-based bots, many of which use network communication features as identifiers of botnet behaviour. In the work of Khattaket al.(2014), the authors have given a detailed review of botnet behaviour, detection and defence. Several studies and researches have been carried out in order to collect and analyse the malware activities like in the work of Baecher et al.(2006), Cooke et al.(2005), and Freiling (2005). A detailed study of botnet activities by a multifaceted approach to collect malware is carried out in the work of Rajab et al. (2006). Detection systems have been developed for different

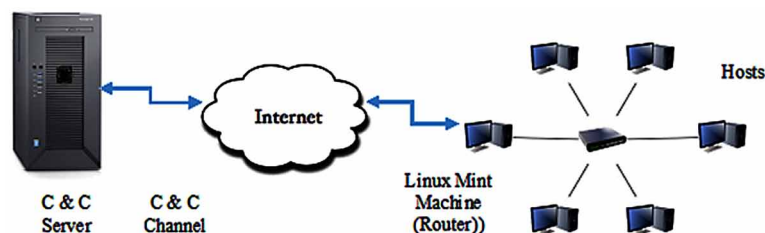
C&C channels such as IRC, as seen in the work of Awadi (2015), HTTP, and P2P. Binsalleeh et al. (2010) present a technical analysis of Zeus crimeware toolkit, which is one of the powerful crimeware tools that emerged in the Internet underground community. Zeus has reportedly infected a large number of computers around the globe. The analysis uncovers the various obfuscation levels and sheds light on the resulting code. Grizzard (2007) provides an overview on the peer-to-peer based architecture of botnets that are most resilient to detection as well as legal shutdowns. A case study of aKademlia based Trojan-Peacomm bot is also presented as an example. In the work of Krmicek et al. (2011), the authors propose DNS flow based techniques for Botnet Detection. Gu et al. (2008) present a general detection framework that is independent of botnet C&C protocol and structure, and requires no prior knowledge of botnets. They define botnet as a coordinated group of malware instances that are controlled via C&C communication channels.

Zhanget al. (2014) propose an approach that uses network based anomaly detection to identify botnet C&C channels in a local area network without any prior knowledge of signatures or C&C server addresses. Strayer et al. (2008) propose a botnet detection approach which examines flow characteristics such as bandwidth, packet timing, and burst duration for evidence of botnet command and control activity. Livadas et al. (2006) propose machine learning techniques to identify the C&C traffic of IRC-based botnet compromised hosts that are collectively commanded using Internet Relay Chat (IRC).

In the work of Perdesci et al. (2010), the authors classify malware according to similarities in URLs extracted from malware HTTP requests. Considering the large number of URLs in the malware traffic, the authors propose a strategy with two steps of clustering process that includes coarse-grained and fine-grained clustering. The authors extract all malware HTTP requests, including both command requests and other benign operations such as connectivity checks. Therefore, their approach in the work is vulnerable to noise injection and malware obfuscation techniques. Another technique is presented in the work of Wurzinger et al. (2009). They extract statefull signatures by observing malware traffic during longer observation periods. It applies the change point detection algorithm on malware traffic in order to detect responses attributable to a command issued by the botmaster. It further analyzes the traffic snippet that just precedes the changing point in order to extract signatures of bot commands. As in the work of Perdesci et al. (2010), the method proposed by Wurzinger et al. (2009) is also vulnerable to noise injection, where a malware hides its change points within the noise traffic so that they are unidentified. There are lot of available literature albeit distantly from our work and those include the work of Li et al. (2006), Yegneswaran et al. (2005), and Newsome et al. (2005), where the network signatures are extracted.

The main challenges with HTTP Botnet detection are the following; first, the botnet communication protocol is very similar to the normal traffic flows, which makes it difficult to identify the botnet communication. These botnets usually get commands by constructing legitimate HTTP requests through the HTTP protocol making it completely stealthy. Second, due to the skewness of botnets in a large network, the volume of malicious traffic generated by botnets is very small. This is because of the rarity of the services offered by botnets like the download of commands whereas the valid and benign HTTP servers contain a variety of services to offer. Hence, there are a large number of HTTP requests from those valid and beneficial services. The HTTP requests from botnets will be too less in number. This limits the identification of bot communication embedded within the large volume of normal traffic. There will be millions of GET requests in which a few tens will be due to HTTP Botnets. It is hence necessary to filter out the benign HTTP flows to analyse the HTTP Botnet traffic flows.

Figure 2. Experimental setup



FOCUS OF THE ARTICLE

System Architecture

Malware analysis plays a significant role in the design of an efficient botnet detection system. Various leaked versions of the bot binaries/builders are taken from Internet and are analyzed on a sandboxed environment and the generated network traffic is captured. The botnet executable files are either directly available or a botnet builder program can be used to build the executable with the required configuration. A typical bot configuration includes C&C server address, update interval, drop name, etc. The bot control panels are hosted using PHP files available with the bot, after editing the database host, username and passwords. The network traffic generated by the bots help to identify the communication pattern and protocol used by the botnet, which may be directly used for implementing a signature based detection system. The system for recording and analysing the HTTP botnet traffic is discussed in this section. Traffic instances are analysed to know the characteristics of botnet communication. Traffic pattern of attack instances are analysed for a specific duration of time. The experimental setup for data capture is shown in figure 2.

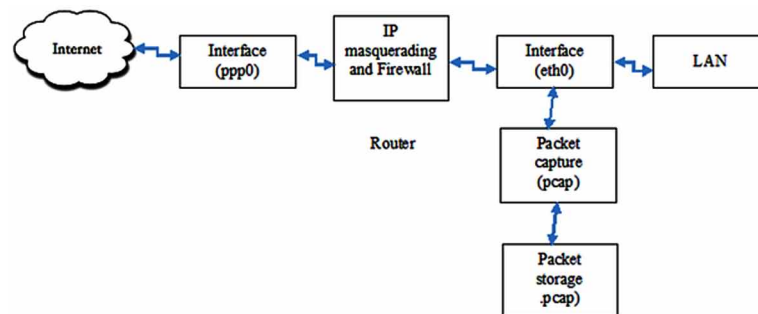
The experimental framework consists of two parts; a local area network and a remote server. The star topology local area network is connected through a border router to the Internet. The switch used in the LAN is an eight port switch. The LAN connects to the Internet through a gateway router as shown in the figure 3. The router consists of two interfaces. IP Masquerading is done along with firewall to set up the router as shown in figure 3. It includes a system for packet capture and for storage. In addition to these hardware components, the framework has components for data capture and analysis.

SOLUTIONS AND RECOMMENDATIONS

System Implementation

The system implemented for the botnet data analysis is explained in this section. The system should essentially include a C&C channel for communication between the bots and the C&C server through a router as shown in figure 2. This setup is achieved by a web server implementation of C&C server and a LAN connecting the bots. The bots are the hosts on the LAN. The remote C&C server is accessed by the bots in the LAN through a router that connects it to the Internet. Each of the components involved are explained in the following subsections.

Figure 3. Diagram showing the block components of router that connects the internet to intranet



C&C Server

The proposed system sets up malwares in a controlled environment. The implementation of malwares is carried out on virtual machines as a security precaution. The C&C channel is of centralised architecture as the botnets setup are HTTP botnets. C&C server is a web server hosted on a Windows 7 machine that is connected to Internet using 4G data card. The web server (C&C Server) is set up using Apache web server along with MySQL. These C&C panels are setup using an open source solution stack package XAMPP. XAMPP is a third party customized software that is completely free, easy to install and manage Apache distribution containing MySQL, PHP, and Perl. Port 80 was kept open for the server to listen to the incoming connections. However, XAMPP comes with its own set of insecurities if not configured properly. A number of C&C panels have been compromised after mapping the XAMPP deployment and exploiting inherent security issues. XAMPP is configured in an open manner to allow developers all flexibility to do anything they want to experiment with.

The missing security features in XAMPP are listed here:

- MySQL administrator has no password.
- MySQL daemon is accessible via network.
- Examples are accessible via network.
- PhpMyAdmin is accessible via network.
- ProFTPD uses the password “lampp” for user “daemon”.

Hence, even a small mis-configuration in deployment of XAMPP could result in serious impacts. In this work XAMPP was configured to listen on machine’s public IP, which was registered with No-IP so that dynamic IP act as static IP by the dynamic DNS service provided by them. The Control Panel and databases for each bot were set up on the server.

Router

The router is set up using Linux Mint machine. Linux Mint is a community-driven Linux distribution based on Debian and Ubuntu that strives to be a “modern, elegant and comfortable operating system, which is both powerful and easy to use”. Two interfaces are needed to configure Linux Mint machine as a router. The two interfaces are classified as internal interface and external interface. Internal interface, i.e. the interface which connects to switch (LAN) is an Ethernet card or LAN card. The external interface

was a 4G data card. The internal interface is referred as eth0 and the external interface is referred to as ppp0 as referred by the Linux machine. Setting up of the router includes the following steps:

1. The decision of the IP range of the LAN and the configuration of internal and external interfaces. The internal interface eth0 is manually set up and the external interface ppp0 is configured automatically as it has DHCP installed in it.
2. IP masquerading is enabled to allow machines with private, non-routable IP addresses on the network to access the Internet through the machine doing the masquerading. Traffic from this network destined for the Internet must be manipulated for replies to be routable back to the machine that made the request. To do this, the kernel must modify the source IP address of each packet so that replies will be routed back to it, rather than to the private IP address that made the request, which is impossible over the Internet. Linux uses Connection Tracking (conn-track) to keep track of which connections belong to which machines and reroute each return packet accordingly. Traffic leaving the private network is thus “masqueraded” as having originated from the Linux Mint gateway machine. This process is referred to in Microsoft documentation as Internet Connection Sharing. IP Masquerading can be achieved by editing the custom ufw rules in the Linux machine

Hosts

Host computers are set up as virtual machines with Windows operating system. These virtual machines run on a Linux platform. The host computers are connected to the network of Linux machines in a bridged mode so that these machines act as a normal system in the network with the same IP range. Hence, these machines could be connected to the switch as in a normal LAN. The virtual machines are chosen to use them as the bot infected machines. The use of virtual machines makes it easy and secure. The LAN interfaces of the hosts need to be configured manually as DHCP server is not installed in the router.

Data Capture

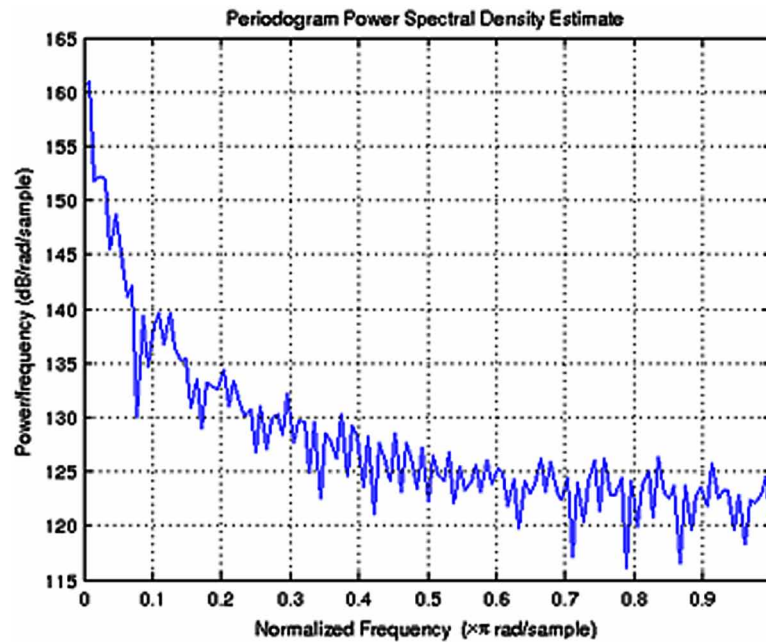
Data capture is done using Wireshark packet sniffer. Wireshark is set to listen to the interface connecting the LAN so that the traffic between the hosts and C&C could be captured. Netflow data is also captured using a software implementation of Netflow probe and a collector program.

Results and Analysis

HTTP botnets named Zeus, Aldi and Umbraloaders are set up and analysed with the framework already discussed.

The Zeus bot client side software is an infection that happens via a drive-by-download, one of the possibly stealthiest forms of infection, or via other means from social media and phishing sites, tempting the user to run an arbitrary executable. Infection can also occur simply through getting access to a computer and using any media for running the bot software. Once infection is successful, the client runs silently on the victim machine, hiding itself to avoid detection. There is no visual sign of this activity to the user. The bot Zeus will delete all the cookies in Internet Explorer and this is to force the user to re-login to the services managed by the user, and also lets Zeus grab the credentials and secret information. The client is configured with a specific time that tells it how often it should run and keep-alive check-ins, update the Command and Control server with new collected information, as well as dynamic configuration updates.

Figure 4. Periodogram of aggregated traffic flow



Aldi Bot is an inexpensive DDoS bot that is growing in popularity. Aldi Bot provides an attacker a simple support mechanism within an organization, which can lead to a much larger security breach. Usually severe attacks involving the exfiltration of sensitive data typically start with one smaller compromise that is then leveraged for additional access like getting a remote or a physical access to a machine by password cracking and then acquiring higher privileges using buffer overflow techniques. Additionally Aldi Bot steals passwords, and passwords are often re-used for convenience for long period of time. Without proper monitoring of system and network activity, such infected nodes can be long-lived and pose significant risk.

The control panel of the HTTP botnets Zeus, Aldi and Umbraloaders is available on the C&C server with various options for attack and stuffs like remove, logout etc. Each communication of Aldi bot contains an HTTP GET request to the C&C server which includes the name, local address, windows version and unique ID generated by the bot. The actual request URL is shown below:

```
/gate.php?hwid=< ID>&pc=<PC NAME>
&localip<IP>=&winver=<WINDOWS VERSION>
```

The botmaster replies with an HTTP OK reply along with text data, which contains commands if any that are issued by the botmaster. When stolen data is exported, a &steal= parameter will be used in the URL that will also include the hwid value as such:

```
gate.php?hwid=<ID>&steal= <URL|USERNAME
|PASSWORD>.
```

The captured data indicates that the bot uses a custom user agent in HTTP requests, “Aldi Bot FTW! :D” and this unknown string can be used for signature based botnet detection.

Umbra Loader C&C panel provides the options for downloading and executing malware, updating bot and uninstalling bot. Each communication session consists of two HTTP POST commands through which the bot connects to the sever using its unique ID and version information. The server does not recognise the internal IP of the infected host in the process. The commands issued by the botmaster are encoded as plain text and appended with the HTTP OK reply for the second POST command. Detailed analysis reveals that the bot uses a custom user agent umbrain the HTTP header and text based data contains a unique ID generated by the bot and a mode number. These features may be used to develop a traffic signature of the bot.

Network traffic analysis is heavily used to detect anomalous and malicious traffic originating from the infected end-user system to C&C panel and vice versa. The analysis shows that HTTP is being used by most of the botnets due to the advantage that most of the traffic in today's web consists of HTTP traffic and it cannot be totally blocked or filtered. A common trend observed among all the analysed bots was that they tend to have a periodic communication with the botmaster and commands are gathered during this phase. The HTTP traffic can be either periodic or non-periodic. That clearly states that periodicity alone is not sufficient for HTTP based botnet detection. However, the periodical pattern communication need to be used as a complementary factor along with other HTTP Botnet detection techniques. Even though periodicity cannot be claimed to be an exclusive feature of bots, they are much common among bots. In order to check periodicity, the periodogram of the traffic flow start time sequence of the aggregated traffic and the normal traffic are plotted. Aggregated traffic included normal and attack traffic. This is shown in the figure4 and figure5 respectively. Comparison between the two periodograms shows that the aggregated traffic exhibits periodicity and hence it can be inferred that the botnet traffic is periodic. Bots were using encrypted communication, which were observed from the traffic traces. This makes it nearly impractical to decode and correlate, hence signature-based techniques would not be sufficient for detection of these bots. Therefore it is better to design a behavioural detection model to detect these bots.

The test data was collected by running the system as pcap files and these files contained the botnet traffic. Using softflowd, Netflow was exported to the local host on a high valued port and collected using the collector program. The periodicity detection algorithm was subsequently applied to the netflow data. The periodicity detection successfully identified the botnet traffic.

Machine learning using random forest was used to model the botnet traffic for an effective detection. There was 100% detection with zero false alerts as shown in table 1. The evaluation metrics are: Precision=1, Recall=1, F-score=1, and Accuracy=100%

FUTURE RESEARCH DIRECTIONS

The HTTP Botnets due to the inherent stealthy behavior, are extremely difficult to be detected. The method of botnet detection using periodicity does not provide a comprehensive solution against HTTP based botnets as periodicity is just one of the characterizing feature of botnets. However, our experimental results show that this approach considerably increases the botnet detection rate on a network. The research to mitigate and prevent botnets is still on a long run, but our solution approach adds a new level of defense.

A common trend observed among all the analyzed bots is that they tend to have a periodic communication with the botmaster and commands are gathered during this phase. This can be used to design behavioural botnet detection model based on periodicity and machine learning techniques. In this work the training of the machine learning algorithm was undertaken on a limited number of samples and as a

Figure 5. Periodogram of the normal traffic flow

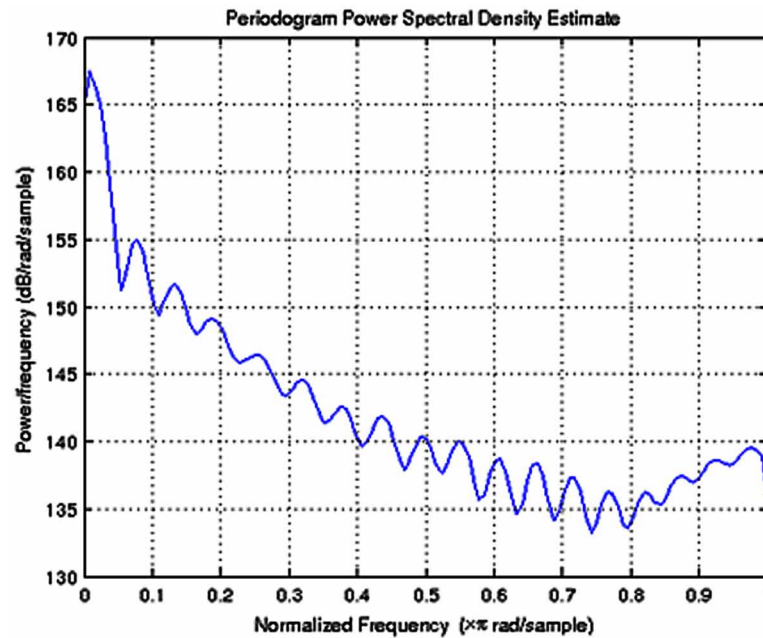


Table 1. Periodicity detection and random forest detection for the botnets

Traffic pattern	Count of bots	Periodicity and Random Forest
Normal	0	NA
Botnet	4	165.254.92.221 to 165.254.145.198 165.254.214.185 to 165.254.145.198 165.254.251.103 to 165.254.145.198 165.254.78.166 to 165.254.145.198

future research more samples need to be collected for building a better model that can detect the novel botnets. It is necessary to include some features other than the periodicity that enable the defenders to better detect the botnets as periodicity does not provide a comprehensive solution against HTTP based botnets.

CONCLUSION

To detect and protect from the attacks caused by botnets, it is important to harness the power of a thorough analysis including periodicity analysis. There are several detection schemes proposed for detecting botnets. This paper proposed an analysis of HTTP botnets by setting the botnets in a controlled environment. Based on the analysis, signature of the bots that were setup is found out. This was used in signature based detection of these bots. In order to detect the new botnets, machine learning classifier using random forest was made use of. The detection of botnets at local networks is possible with this simple work where the botnet infected client machines are detected and hence eliminated from the net-

work. The results demonstrated the higher detection of botnets using periodicity analysis and machine learning techniques.

REFERENCES

- AsSadhan, B., Moura, J.M.F., & Lapsley, D. (2009). Periodic Behavior in Botnet Command and Control Channels Traffic. *Proceedings of the IEEE Global Telecommunications Conference*, 1-6.
- Awadi, H. R. A., & Belaton, B. (2015). Multi-phase IRC Botnet and Botnet Behavior Detection Model. *ArXiv e-prints*.
- Baecher, P., Koetter, M., Holz, T., Dornseif, M., & Freiling, F. C. (2006). The nepenthes platform: An efficient approach to collect malware. *Lecture Notes in Computer Science*, 4219, 165–184.
- Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010). On the analysis of the zeus botnet crimeware toolkit. In *Privacy Security and Trust (PST). Eighth Annual International Conference*, 31–38.
- Cooke, E., & Jahanian, F. (2005). The zombie roundup: Understanding, detecting, and disrupting botnets. In D. Katabi & B. Krishnamurthy (Eds.), *SRUTI. USENIX Association*.
- Freiling, F. C., Holz, T., & Wicherski, G. (2005) Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. *Lecture Notes in Computer Science*, 3679, 319–335.
- Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., & Dagon, D. (2007). Peer-to-peer botnets: Overview and case study. In N. Provos (Ed.), *HotBots. USENIX Association*.
- Gu, G., Perdisci, R., Zhang, J., & Lee, W. (2008). Botminer: Clustering analysis of network traffic for protocol - and structure independent botnet detection. *USENIX Security Symposium*, 139–154.
- Gu, G., Zhang, J., & Lee, W. (2008). Botsniffer: Detecting botnet command and control channels in network traffic. *NDSS The Internet Society*.
- Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. (2014). A taxonomy of bot-net behavior, detection, and defense. *IEEE Communications Surveys and Tutorials*, 16(2), 898–924. doi:10.1109/SURV.2013.091213.00134
- Krmicek, V. (2011). Inspecting DNS flow traffic for purposes of botnet detection. *GEANT3 JRA2 T4 Internal Deliverable*, 1-9.
- Li, Z., Sanghi, M., Chen, Y., Kao, Y. M., & Chavez, B. (2006). Hamsa: Fast signature generation for zero-day polymorphic worms with provable attack resilience. *IEEE Symposium on Security and Privacy*.
- Livadas, C., Walsh, R., Lapsley, D., & Strayer, W. (2006). Using machine learning techniques to identify botnet traffic. *Local Computer Networks, Proceedings of the 31st IEEE Conference on*, 967–974.
- Newsome, J., Karp, B., & Song, D. (2005). Polygraph: Automatically generating signatures for polymorphic worms. *IEEE Symposium on Security and Privacy*. 10.1109/SP.2005.15

Perdisci, R., Lee, W., & Feamster, N. (2010). Behavioral clustering of http-based malware and signature generation using malicious network traces. *USENIX Symposium on Networked Systems Design and Implementation*.

Rajab, M. A., Zarfoss, J., Monroe, F., & Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 41–52. 10.1145/1177080.1177086

Strayer, W. T., Lapsley, D. E., Walsh, R., & Livadas, C. (2008). Botnet detection based on network behavior. *Springer Advances in Information Security*, 36, 1–24.

Wurzinger, P., Bilge, L., Holz, T., Goebel, J., Kruegel, C., & Kirda, E. (2009). Automatically Generating Models for Botnet Detection. *LNCS*, 5789, 232–249. doi:10.1007/978-3-642-04444-1_15

Yegneswaran, V., Giffin, J. T., Barford, P., & Jha, S. (2005). An architecture for generating semantic-aware signatures. *USENIX Security Symposium*.

Yu, S., Guo, S., & Stojmenovic, I. (2015). Fool me if you can: Mimicking attacks and anti-attacks in cyberspace. *Computers. IEEE Transactions on*, 64(1), 139–151.

Zhang, J., Perdisci, R., Lee, W., Luo, X., & Sarfraz, U. (2014). Building a scalable system for stealthy P2P-botnet detection. *Information Forensics and Security, IEEE Transactions on*, 9(1), 27–38.

ADDITIONAL READING

Acarali, D., Rajarajan, M., Komninos, N., & Herwono, I. (2016). Survey of approaches and features for the identification of HTTP-based Botnet traffic. *Journal of Network and Computer Applications*, 76, 1–15. doi:10.1016/j.jnca.2016.10.007

Aziz, A. S. A., Hanafi, S. E. L.-O., & Hassanien, A. E. (2017). Comparison of Classification Techniques Applied for Network Intrusion Detection and Classification. *Journal of Applied Logic*, 24, 109–118. doi:10.1016/j.jal.2016.11.018

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, 50(2), 76–79. doi:10.1109/MC.2017.62

Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5–32. doi:10.1023/A:1010933404324

Chen, C.-M., & Lin, H.-C. (2015). Detecting Botnet by anomalous traffic. *J Inform Secur Appl*, 21, 42–51.

Chen, W., Luo, X., Yin, C., Xiao, B., Au, M. H., & Tang, Y. (2017). CloudBot: Advanced mobile Botnets using ubiquitous cloud technologies. *Pervasive and Mobile Computing*, 41, 270–285. doi:10.1016/j.pmcj.2017.03.007

Huang, C.-Y. (2013). Effective bot host detection based on network failure models. *Computer Networks*, 57(2), 514–525. doi:10.1016/j.comnet.2012.07.018

Robinson, R.R.R., Thomas, C. (2015). Ranking of machine learning algorithms based on the performance in classifying DDoS attacks. *IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, 185–190.

Wang, K., Huang, C.-Y., Lin, S.-J., & Lin, Y.-D. (2011). A fuzzy pattern-based filtering algorithm for Botnet detection. *Computer Networks*, 55(15), 3275–3286. doi:10.1016/j.comnet.2011.05.026

KEY TERMS AND DEFINITIONS

Botmaster: Botmaster is the master of bots on the network. A botmaster is responsible for keeping the bot online, sending control commands to bots for its operation, making sure to fix issues with bots, and set a set of rules for bots to function.

Botnet: A botnet is a collection of bots. Botnets originate many types of attacks like distributed denial-of-service attack (DDoS attack), data theft, spamming, and intrusion to systems and networks.

Bots: Any system connected to Internet becomes a bot when it runs automated tasks or scripts over the internet. Majority of the malicious web traffic gets originated from bots.

C&C Server: A command and control server (C&C server) is a system that issues directives to other connected systems that have been infected with rootkits or other types of malware such as ransomware.

Firewall: A firewall is a network security system that allows or denies incoming and outgoing network traffic based on predetermined security rules.

HTTP: HTTP means HyperText Transfer Protocol. HTTP is the underlying protocol used by the world wide web and this protocol defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

Intrusion Detection Systems: An intrusion detection system (IDS) is a hardware device or software application that monitors a network or systems for malicious activity or policy violations.

IRC: Internet relay chat (IRC) is a system for chatting that involves a set of rules and conventions and client/server software.

Periodicity: Periodicity is the occurrence of similarity in more or less regular intervals and is a property exhibited by many processes that are of interest in a variety of scientific disciplines.

Random Forest Classifier: Random forest classifier uses a set of decision trees from randomly selected subset of the training data and then aggregates the decision from each set to arrive at the final decision class of the test data. This improves accuracy and avoids over-fitting and hence better than decision tree algorithms.

Router: Router is an inter-networking device that forwards the packets from one computer network to another. Routers perform the traffic route finding on the Internet by means of a routing table.

Signature-Based Classifier: Signature-based classifier classifies items based on an entry in a lookup table with signatures and the corresponding class labels. Hence, this classifier is not efficient in detecting novel patterns/signatures.

Hybrid Artificially Intelligent Multi-Layer Blockchain and Bitcoin Cryptology (AI-MLBBC): Anti-Crime-Theft Smart Wall Defense

Murad Al Shibli

Abu Dhabi Polytechnic, UAE

INTRODUCTION

This chapter presents an integrated secured framework of blockchain and bitcoin cryptology with the artificial intelligence of neural networks and machine learning. Recently blockchain has been received special attention and used as a new platform for digital information and to store encrypted data and process secure digital transactions. Noticeably, the majority of blockchain cryptocurrency technology is structured based on the elliptic curves digital signature algorithm (ECDSA). In particular, Bitcoin uses special elliptic curves digital signature algorithm (ECDSA) called secp256k1. Losses of personal and organizational data have been reported and occurred due to security breaches of data at minor and major scales using traditional transactional and financial platforms. Furthermore, data on blockchain and Bitcoin platforms are assumed to be highly encrypted and secured state. This feature enable blockchain to be an ideal system to save confidential and personal data as well as sensitive organizational and financial information. Although blockchain and bitcoin databases are encrypted using private keys, but there are many cryptocurrency bitcoin wallets have been reported hacked which resulted in losing millions of dollars. Breaching blockchain can lead to exposing sensitive data to high risk. The artificial intelligent neural networks (AINN) algorithms possess the capability features of processing and operating encrypted data and will lead to minimal risk. Pretrained convolutional neural network (CNN) training is proposed to be implemented a part of the block chain to protect personal data and information as third wall defense against hacking. CCN is used to extract learned image features and use those features to train an image classifier with single pass making advantage of machine learning tools features.

In this chapter presents a literature survey is presented, mathematical background of elliptic curves for real and finite prime fields is introduced, elliptic curves cryptosystem is addressed, and bitcoin digital signatures are demonstrated. Moreover, a novel integrated cryptology approach of artificial intelligence based blockchain and bitcoins by introducing a multilayer security layer and neural networks machine learning and big data mining. Specifically, this revolutionary safe combination criteria is structured by implementing a coupled private key elliptic curves digital signature in order to securely enter into the blockchain and process encrypted data using neural networks. Furtherly, encrypted big data can be processed by neural networks linear regression and out-of-memory tall arrays criteria. Moreover, artificial intelligent machine learning of photography can be encrypted-decrypted by using a pertained Convolutional Neural Networks (CNN) and by utilizing Singular Value Decomposition (SVD) and XOR-Secret cipher key.

DOI: 10.4018/978-1-5225-9715-5.ch075

In this chapter, Section 1 will introduce a literature survey, Elliptic Curves Defined Over Real Field is presented in Section 2, Elliptic Curves Cryptosystem Over Finite Prime Fields is introduced in Section 3, Elliptic Curve Cryptographic Algorithm is addressed in section 4, moreover, Bitcoin Elliptic Digital Signature Cryptosystem is presented in Section 5, Multilayer Elliptic Curve Digital Signatures are introduced in Section 6. Moreover, Protection of Data Using Pretrained Convolutional Neural Network (CNN) and Singular Value Decomposition (SVD) is proposed in Section 7 along with simulations results. Finally, conclusions are drawn in Section 8.

BACKGROUND

In 2008, Bitcoin was introduced for the first time by Satoshi (2008) as a new type of crypto-currency. Bitcoin as a peer-to-peer digital transaction is structured based on non-centralized chain that is not governed by any central financial bank or any government. Nakamoto proposed to use cryptographic transactions to allow any two parties to transact directly with each other without going through the traditional practice of a trusted third party. Due to this new concept and it has been public used worldwide. The mathematical algorithm and transactions of Bitcoins are built based on elliptic curves. An overview of Digital Signature Algorithm (DSA) and its Elliptic Curve Digital Signature Analogue (ECDSA) and related application in the blockchain and Bitcoin technologies are presented in article of Kikwai (2017). To ensure high security levels for users recommended Elliptic Curve Domain Parameters (ECDP) are introduced in the research work reported by Brown doe SEC1 in (2009) and for SEC2 in (2009). The Wireless Application Forum (2001) has developed the wireless transport layer security and associated wireless application protocol WAP-261-WTLS-20010406-a in order to provide privacy, data integrity and secure authentication between two communicating applications. The American National Standards Institute (2001) and (2005) has identified methods to generate and verify digital signature to secure messages and data using ECDSA in two published standards. These curves and parameters are derived based on Elliptic Curve Cryptography regulated by Standards for Efficient Cryptography Group, ANSI and IEEE.

Multiple elliptic curves digital signature algorithm is proposed in research of Bi, Jia & Zheng, (2018). This algorithm will allow selecting many elliptic curves and editing elliptic curve parameters. This scheme is shown to be secure and efficient with two elliptic curves as recommended. Important questions about Bitcoin are addressed in the book published by (Narayanan, Bonneau, Felten, Miller & Goldfeder, 2016). It addresses the principles of Bitcoin, what makes it different, how bitcoins are anonymous, associated applications, regulations, and future trends. An overview of a bitcoin digital transactions is presented in the thesis work of Crossen, S. (2015). Individual transaction details and security, associated blocks as well as Bitcoin public ledger are highlighted along with mathematical Elliptic Curve background. Elliptic Curve Cryptography using the secp256k1 curve, Elliptic Curve Digital Signature Algorithm, and Secure Hash Algorithm 256 (SHA256) are also discussed. Research work reported by (Haddaji, Ouni, Bouaziz & Mtibaa, 2016) addresses the benefits of the implementations of the electronic signature ECDSA compared to the digital signature algorithm (DSA) used to authenticate compressed videos of H.264. The added value of this algorithm is tested on a set of videos to compare strength, add-time, speed, number of gates of some hashed videos using MD5 functions. The research work Ghosh & Nath, (Nov. 2014) presents a theoretical study of data encryption using artificial neural networks (ANN) using Neural Cryptography. Using feedback, ANN is used to produce efficient data encryption systems.

ANN composed of one or multilayer perceptron models are reported to be more efficient in encrypting systems based on feedback in the field of cryptography.

Bitcoin systematic analysis of broken primitives are presented by (Giechaskiel, Cremers & Rasmussen, Feb. 2016) in which Cryptographic blocks and related effect on the Bitcoin security are identified. Primitive breakage range of simple privacy violations and full breakdown of the bitcoin currency analysis is revealed. Many findings and recommendations for Bitcoin threat of broken cryptographic primitives are introduced. Unique mistakes and vulnerabilities associated to the implementations elliptic curve cryptography (ECC), are reviewed and revealed unique published by Bos, Halderman, Heninger, Moore, Naehrig, & Wustrow (March 2014). Bitcoin and other protocols such as secure shell (SSH) and transport layer security (TLS), and Austrian e-ID are studied. It is found that only 10% of the systems support ECC and vulnerabilities are highly exposed.

The concept of Elliptic Curve Digital Signature Algorithm (ECDSA), its mathematical context and successful practice methods are introduced by Linke (May 2014). ECDSA is considered as asymmetric authentication systems which is based on a private key at authenticator level and another public key used at host level to validate the authentication. On the other hand, the symmetric authentication scheme systems used a common secret keys shared by both the user and host. Accelerated verification scheme of Elliptic Curve Digital Signature Algorithm (ECDSA) in wireless sensor networks (WSN) is proposed by Kheradmand (2013). The delay is due to the fact that ECDSA requires an extra point and two multi scalars to verify WSN signature. If cooperation among sensor nodes is exploited then the delay can be solved. A new efficient and optimal scheme is proposed to provide a threshold DSA/ECDSA algorithm proposed by (Gennaro1, Goldfeder & Narayanan, 2016). This algorithm will enhance the security of Bitcoin wallets to avoid any thefts. Implementation of elliptic curve P-192 with ANSI X9.62 ECDSA and associated security is described in the work of (Khalique, Singh & Sood, 2010). The adoption of ECDSA as a standard at ISO, ANSI, IEEE and NIST is reported in 1998, 1999, 2000, and 2000, respectively.

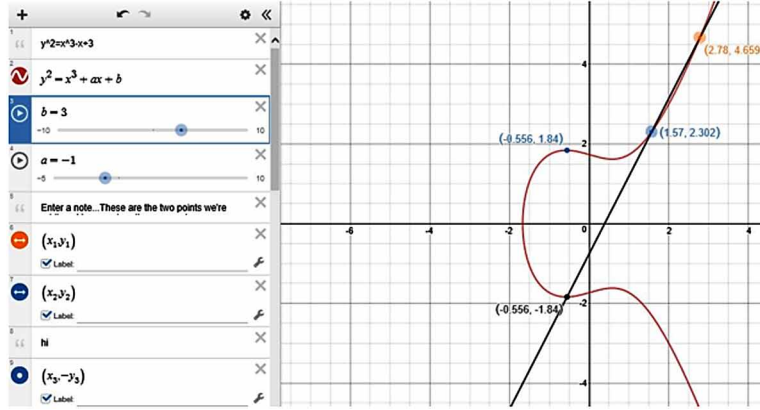
Elliptic Curve Cryptography backgrounded with text and imaged background implementation is briefed in the paper of (Kolhekar & Jadhav, July 2011). This is due to the robustness and security of the mathematical compared to other schemes. Prediction of future facts of the Ethereum blockchain can be explored by Deep Learning (DL) methods is reported by (Besarabov & Kolev, 2018). This prediction approach is implemented by using as the transaction count and the account balance distributions. DL is performed to create reusable blockchain framework to provide data, processing and storage. New US patents on blockchain-enabled peer-to-peer drone delivery service, cloud, satellite networking services and cryptocurrency are reported by Al-Shibli (2019).

ELLIPTIC CURVES DEFINED OVER REAL FIELD

Elliptic curves are defined by cubic equations and are totally different from ellipses or ellipsoids. In a two dimensional plane, the elliptic curve E is a cubic curve described over a real domain $\mathbf{R}$ whose points satisfy the following Weierstarss equation

$$E: y^2 + axy + by = x^3 + cx + d \quad (1)$$

where x and y take on values in the real number field, and the coefficients a , b , c , d are all have real number values. For the purpose of applicability, it is very common reduce the Elliptic curves introduced in Equation (1) to have the following reduced form

Figure 1. Elliptic curve plot over $\mathbf{R}$ for: $y^2=x^3-x+3$ ($a = -1$, $b = 3$)

$$E: y^2 = x^3 + ax + b \quad (2)$$

Because the highest order (exponent) is 3, the elliptic curves are said to be cubic equations. Moreover, a zero point is defined with an elliptic curve as a single element denoted O (also called the point at infinity). In order to plot the elliptic associated curve, Equation (2) can be put in the square root form as:

$$y = \sqrt{x^3 + ax + b} \quad (3)$$

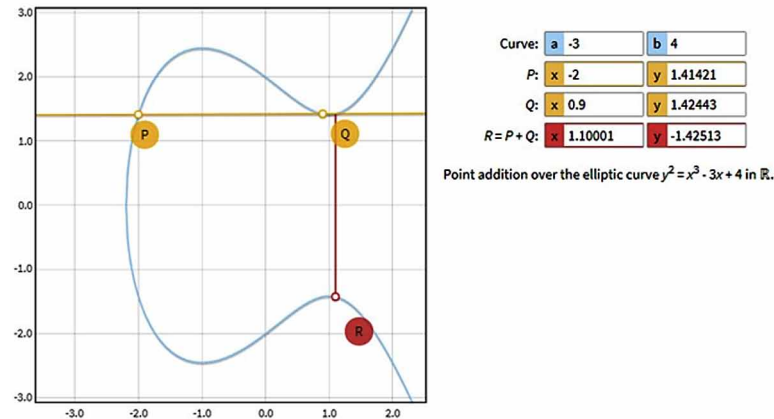
For every value of x in Equation (3), negative values of y plot are obtained if specific values of a and b are used. For every quadratic residue x of the elliptic curve defined in (3), there are two solutions exist: y and $-y$ exist. Examining elliptic curves is found that the associated plots are symmetric about x -axis ($y=0$). Because of this symmetric property, for every point $P=(x,y)$, there is a negative or inverse negative point $-P=(x,-y)$ such that $P+(-P)=O$. The identity point O can now be added to the elliptic curves group definition such that the group elements can be defined for all points (x,y) on some elliptic curve $=x^3+ax+b$, and the identity point O . This leads to what is called as an infinite group.

Furthermore, the identity point O and all points on located on an elliptic curve form cyclic subgroups.

It is reported that arithmetic operations of elliptic curves over real domains $\mathbf{R}$ usually leads to irrational numbers and computer truncation errors that and improper memory storage. Therefore, it is recommended to work over finite prime fields associated with elliptic curves. A finite prime field of order q such that $q=p^k$ in which p is a prime and p and k are integers that satisfy the modified original Equation (2) given a domain parameters over $\mathbf{F}_q: T=(q,a,b,G,n,h)$

$$y^2 = x^3 + ax + b \pmod{p} \quad (4)$$

Equation (4) of an integer p identifying the finite prime field $\mathbf{F}_q$, given that $4a^3+27b \not\equiv 0 \pmod{p}$, where p is a large prime. The two coefficients $a, b \in \mathbf{F}_q$, specifying an elliptic curve $E(\mathbf{F}_q)$ defined in Equation (4) with randomly selected elements on $E(\mathbf{F}_q)$ called a base point $G=(x_G, y_G)$. The base point G has an order n which is a large prime that yields $nG=O$ which is defined earlier as the zero element of the field such that $n > 4\sqrt{p}$ and $n > 2^{160}$. The cofactor h is an integer that satisfies $h \neq E(\mathbf{F}_q)/n$. Moreover, the non-singularity condition $4a^3+27b$ meant not to be congruent to 0 modulo p .

Figure 2. Point addition over the elliptic curve: $y^2 = x^3 - 3x + 4$ ($a = -3$, $b = 4$)


The elliptic equation described in (2) should satisfy the condition $p \neq 2$. In case that $p = 2$, then Equation (4) will yield to the form:

$$y^2 + xy = x^3 + ax + b \quad (5)$$

Over $\mathbb{R}$, there is a natural geometric construction that transforms the points of an elliptic curve into an abelian group having O as the neutral element. In this addition of points will be expressed for two points as follows. The addition for a group operation on $E(\mathbb{F}_q)$ of two points: $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, an additive third point $P_3 = (x_3, y_3) = P_1 + P_2$

$$x^3 = s^2 - x_1 - x_2 \dots \dots \text{mod } p \quad (6)$$

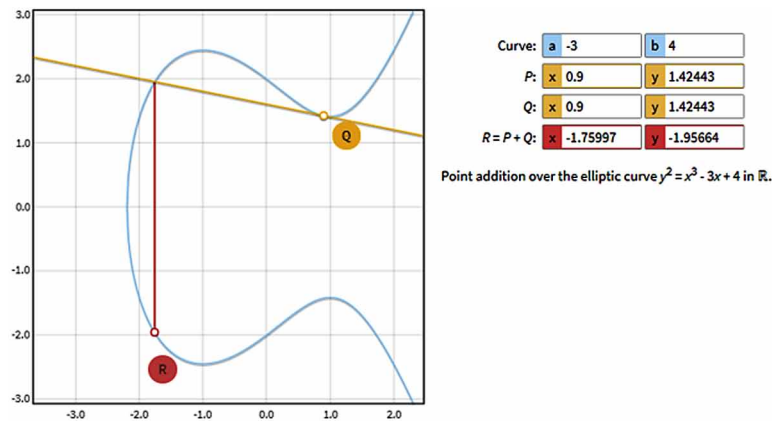
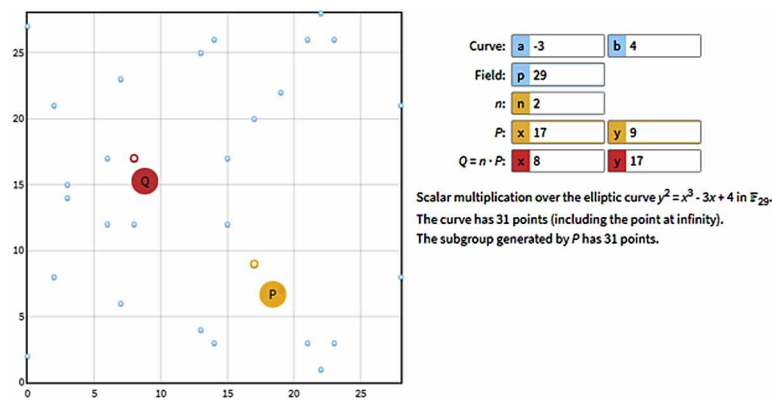
$$y_3 = s(x_1 - x_3) - y_1 \dots \dots \text{mod } p \quad (7)$$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \text{mod } p, P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} \text{mod } p, P_1 = P_2 \end{cases} \quad (8)$$

It is interested to know the total number of points (N) of an elliptic curve given modulo p . It is found that N is almost nearby the prime p as follows:

$$p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p} \quad (9)$$

adding two points $P + Q = R = (-2.0, 1.4) + (0.9, 1.4) = (1.1, -1.4)$ doubling a point $A + A = 2 * (0.9, 1.42) = (-1.76, -1.96)$

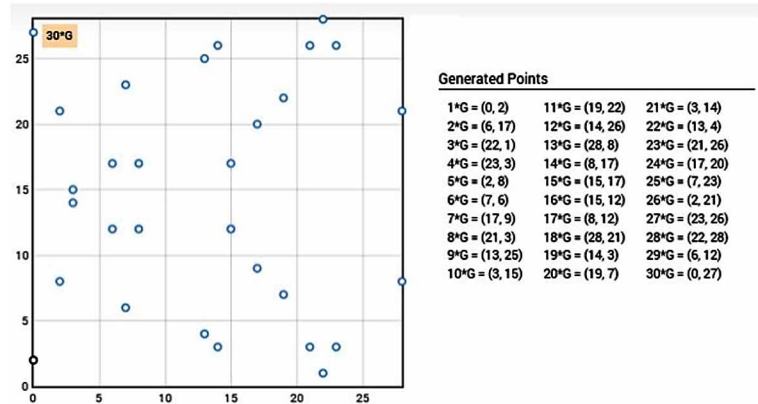
Figure 3. Scalar multiplication over the elliptic curve in real field R for $y^2 = x^3 - 3x + 4$ Figure 4: Doubling a Point of an Elliptic Curve in Finite Prime Field F : $y^2 = x^3 - 3x + 4$ 

ELLIPTIC CURVES CRYPTOSYSTEM OVER FINITE PRIME FIELDS

The entire group of an elliptic curve $E(\mathbb{F}_q)$ is not practically needed as a whole, instead a cyclic subgroup is sufficient. A sufficient large cyclic subgroup of $E(\mathbb{F}_q)$ can be generated by selecting the parameters: a, b, p, k and base point $G \in E(\mathbb{F}_q)$. These parameters are shared publicly in Elliptic Curves cryptosystem and used to produce public keys. In general it is assumed that any point P on the elliptic curve can be generated and expressed in terms of the base point G and a non-negative integer n as follows:

$$P = G + G + \dots + G = nG \quad (10)$$

Based on the Equation (10), it is easy to calculate the new point P provided a base point G and an integer n . But on the other hand, it is very hard and infeasible to do the opposite and find the integer n given the point $P = nG$. Furthermore, double and add scheme is defined for an elliptic curve group element P and n is an integer, then $n \cdot P$ is a multiple copies of the base point P added together using point addition. Figures 4 and 6 demonstrates some examples of doubling and multiples of Elliptic Curve in Finite Prime Field. Doubling a point $P + P = Q = 2 * (17, 9) = (8, 17)$

Figure 5. Multiples of the base point $P(0, 2.0)$ over the Prime Field: $y^2 = x^3 - 3x + 4$ with Modulus 29

ELLIPTIC CURVE CRYPTOGRAPHIC ALGORITHM

In order to perform a successful and secure elliptic curve cryptographic algorithm, the following parameters are required:

1. A finite elliptic cubic curve coefficients a and b ;
2. A finite prime modulus p ;
3. A base point $G=(x,y)$ with which point multiplication will be performed such that $n \cdot P = O$. The order of G is identified by the value n . It should be noted that n must be a large prime number. The size of n determines the level of the security.

Hash Function: Hash function H is very important to create and verify a digital signature. It is defined as an effective computational function that needed to map a random length binary string to a fixed length binary string. Hash function H should meet the following technical specifications:

1. **Collision Resistance:** An infeasible computational condition to find two distinct inputs r_1 and r_2 such that $H(r_1) = H(r_2)$;
2. **First Pre-Image Resistance:** For any given output z it is not feasible to find an input such that $H(r) = z$.
3. **Second Pre-Image Resistance:** An infeasible computational condition for a given input message r to another inputs r' such that $H(r) = H(r')$;

This is crucially important for digital signatures as primitive cryptographic that is based on authentications, authorization and non-rejection.

Figure 6. Bitcoin elliptic curve plot over $R: y^2=x^3+7$ ($a = 0, b = 7$)

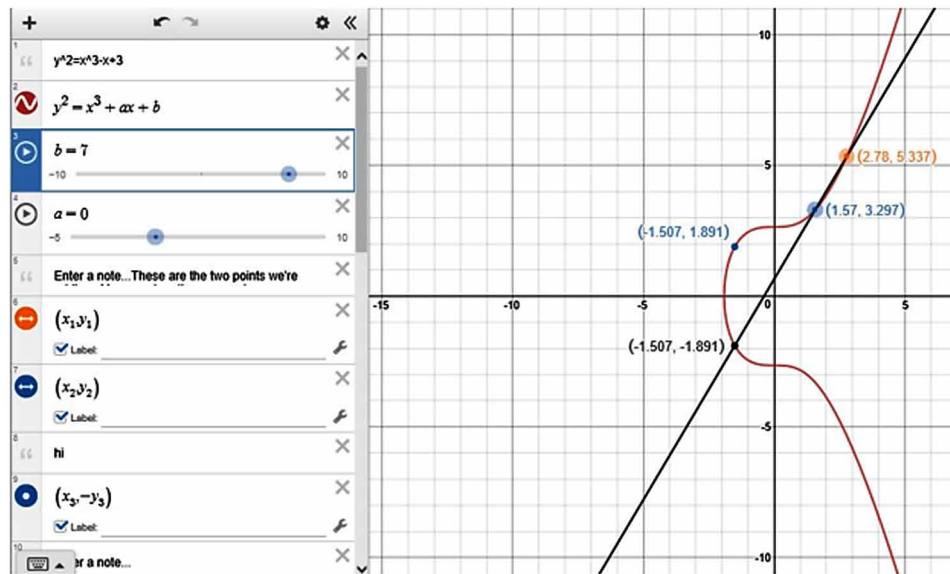
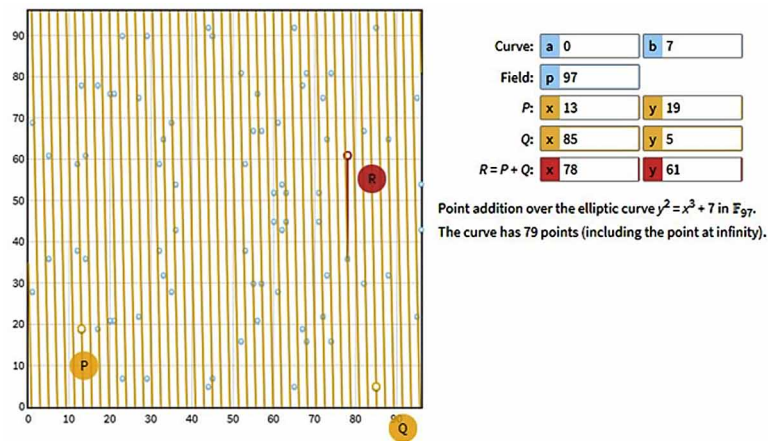


Figure 7. Bitcoin point addition over the finite prime field for $y^2=x^3+7 \bmod 97$



BITCOIN ELLIPTIC DIGITAL SIGNATURE CRYPTOSYSTEM

The Bitcoin invented by Satohsi Nakamoto is defined over a finite prime field of order q such that $q=p^k$ in which p is a prime and p and k are integers that satisfy the Equation (2) given a domain parameters over $\mathbb{F}_q: T(p,a,b,G,n,h)$

$$y^2 = x^3 + 7 \pmod{p} \quad (11)$$

Figure 6 demonstrates the plot of the Bitcoin Elliptic Curve over $\mathbb{R}$: $y^2 = x^3 + 7$ ($a = 0, b = 7$). On the other hand, plotting Bitcoin Finite Prime Field to display addition of points with a given modulus is shown in Figure 7. adding points $P(13,19) + Q(85,5) = R(78,61)$

Bitcoin Digital Algorithm

Define an elliptic curves digital signature algorithm (ECDSA) such that: $y^2 = x^3 + 7 \pmod{p}$.

A signer selects a random number $m \in [1, n]$ as a private key and calculate a public key $q = mG$

Phase 1: ECDSA Signature Generation: An initiator sends a message M as follows:

- Step 1: Compute a secure hash H such that $e = H(M)$;
- Step 2: Choose a random cryptographic integer k from the range $[1, n - 1]$ and then calculate $kP = (x, y)$;
- Step 3: Calculate r such that $r = x \pmod{n}$ and not to be zero. If zero, then go back to step 2.
- Step 4: Compute $s = k^{-1}(e + mr) \pmod{n}$;

Output: The cryptographic signature is (r, s) .

Phase 2: ECDSA Signature Verification: A receiver can check if the message M is true as follows:

- Step 1: Check that r and s are integers in $[1, n - 1]$, if not then the signature is not valid.
- Step 2: Calculate the hash H such that $e = H(M)$ as in phase 1.
- Step 3: Determine w as $w = s^{-1} \pmod{n}$;
- Step 4: Compute $u = ew \pmod{n}$ and $v = rw \pmod{n}$;
- Step 5: Obtain $R = uP + vQ = (x, y)$;

Output: The signature is valid if only if $r = (x \pmod{n})$. Otherwise it is not valid.

The modulus, base point, public key and private keys are demonstrated in Figure 8 and 9 of bitcoin digital signature.

ECDSA Signature

secp256k1 (Bitcoin): $y^2 = x^3 + 7 \pmod{p}$.

$$P = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^5 - 2^4 - 1;$$

$P = 115792089237316195423570985008687907853269984665640564039457584007908834671663$
 $G_x = 0x79BE667E F9DCBBAC55 A06295CE87 0B07029BFC DB2DCE28D9 59F2815B16 F81798$
 $G_y = 0x483ADA77 26A3C4655D A4FBFC0E11 08A8FD17B4 48A6855419 9C47D08FFB 10D4B8$

Public Key

x : 3987461777 6630327813 1900584138 1656076773 4954098998 5670432249 5007453314 3699292
 y : 83115399533 2222005344 4205005182 6386603242 6099204094 3062687608 0623730665 355556

Figure 8. Bitcoin public key generation using python code

```

1 # Hello world program in Python
2
3 """
4 Calculations on the secp256k1 curve work.
5
6 secp256k1 is the name of the elliptic curve used by bitcoin
7
8 see http://bitcoin.stackexchange.com/questions/25382
9
10 """
11 p = 2**256 - 2**32 - 977
12
13 def inverse(x, p):
14     """
15     Calculate the modular inverse of x ( mod p )
16
17     the modular inverse is a number such that:
18
19     (inverse(x, p) * x) % p == 1
20
21     you could think of this as: 1/x
22     """
23     inv1 = 1
24     inv2 = 0
25     while p != 1 and p!=0:
26         inv1, inv2 = inv2, inv1 - inv2 * (x / p)
27         x, p = p, x % p
28     return inv2
29
30
31
32 def dblpt(pt, p):
33     """
34     Calculate pt+pt = 2*pt
35     """
36     if pt is None:
37         return None
38     (x,y)= pt
39     if y==0:

```

Figure 9. Bitcoin public key output using python code

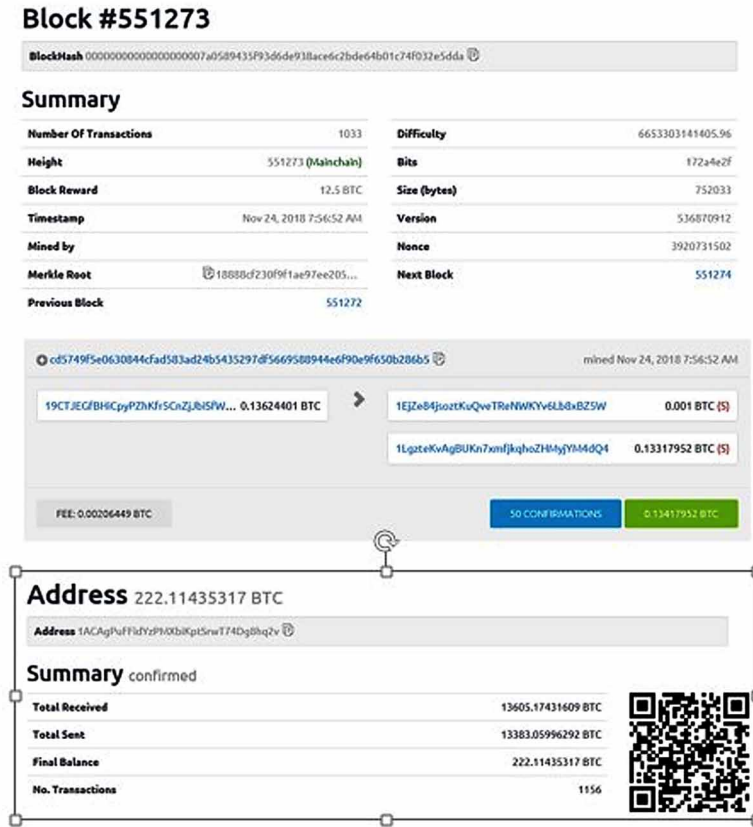
```

Python Code Output:
2*G= (c6047f9441ed7d6d3045406e95c07cd85c778e4b8cef3ca7abac09b95c709ee5, 1ae168
fea63dc339a3c58419466ceaeef7f632653266d0e1236431a950cfe52a)

G+2*G= (f9308a019258c31049344f85f89d5229b531c845836f99b08601f113bce036f9, 388f
7b0f632de8140fe337e62a37f3566500a99934c2231b6cb9fd7584b8e672)
2*G+2*G= (e493dbf1c10d80f3581e4904930b1404cc6c13900ee0758474fa94abe8c4cd13, 51
ed993ea0d455b75642e2098ea51448d967ae33bfbdfef40cfe97bdc47739922)

pubkey= (71ee918bc19bb566e3a5f12c0cd0de620bec1025da6e98951355ebbde8727be3, 37b
3650efad4190b7328b1156304f2e9e23dbb7f2da50999dde50ea73b4c2688)

```

Figure 10. An example of a real bitcoin transaction on <https://blockexplorer.com/>

Signature

r : 2528236291 5497655056 3295129171 2165408860 2539327808 2160772679 3641177999 6643728
 s : 39257440409 4909346526 4458985977 1879805788 2410643514 6173830707 3788061051 966857

MULTILAYER ELLIPTIC CURVE DIGITAL SIGNATURES

This section aims to generalize using multiple elliptic curve signature to ensure a double security [4]. A combination of two or more signature can be used. For the purpose of generality, the elliptic curve domain parameters over a finite field $\mathbf{F}_q$ is defined by:

$$T = (q, A, B, C, n, H) \quad (12)$$

such that q is an integer specifying the finite field $\mathbf{F}_q$, two parameters $A, B \in \mathbf{F}_q$, and C is a base point $C = (x_c, y_c)$ exists on $E(\mathbf{F}_q)$ with a prime n as the order of C and an integer cofactor H such that $H \neq E(\mathbf{F}_q)/n$. All specifying an elliptic curve $E(\mathbf{F}_q)$ defined by the equation:

$$y^2 = x^3 + Ax + B \pmod{p} \quad (13)$$

Table 1. Recommended Parameters of secp192k1

secp192k1	
The Curve Equation	$y^2 = x^3 + 3 \pmod{p}$
q	= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFEE37 = $2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$
A	= 00000000 00000000 00000000 00000000 00000000 00000000
B	= 00000000 00000000 00000000 00000000 00000000 00000003
C	= 03 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D (Compressed) = 04 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D 9B2F2F6D 9C5628A7 844163D0 15BE8634 4082AA88 D95E2F9D (Uncompressed)
n	= FFFFFFFF FFFFFFFF FFFFFFFF 26F2FC17 0F69466A 74DEFD8D
H	= 01

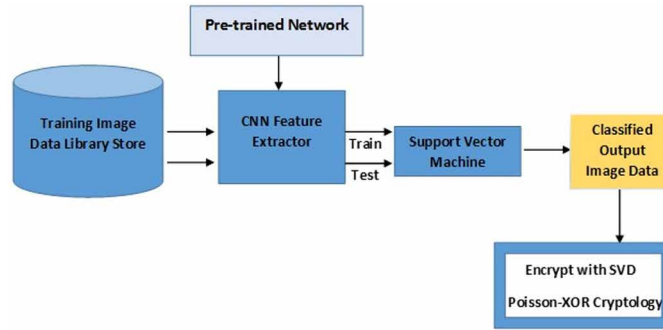
Table 2. Recommended Parameters of Secp224k1

Secp224k1	
The Curve Equation	$y^2 = x^3 + 5 \pmod{p}$
q	= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFEE56D = $2^{224} - 2^{32} - 2^{12} - 2^{11} - 2^9 - 2^7 - 2^4 - 2 - 1$
A	= 00000000 00000000 00000000 00000000 00000000 00000000 00000000
B	= 00000000 00000000 00000000 00000000 00000000 00000000 00000005
C	= 03 A1455B33 4DF099DF 30FC28A1 69A467E9 E47075A9 0F7E650E B6B7A45C (Compressed) = 04 A1455B33 4DF099DF 30FC28A1 69A467E9 E47075A9 0F7E650E B6B7A45C 7E089FED 7FBA3442 82CAFBDB F7E319F7 C0B0BD59 E2CA4BDB 556D61A5 (Uncompressed)
n	= 01 00000000 00000000 00000000 0001DCE8 D2EC6184 CAF0A971 769FB1F7
H	= 01

Table 3. Recommended Parameters of Secp256k1

Secp256k1	
The Curve Equation	$y^2 = x^3 + 7 \pmod{p}$
q	= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F = $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
A	= 00000000 00000000 00000000 00000000 00000000 00000000 00000000
B	= 00000000 00000000 00000000 00000000 00000000 00000000 00000007
C	= 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 (Compressed) = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8 (Uncompressed)
n	= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF BAAEDCE6 AF48A03B BFD25E8C D0364141
H	= 01

Figure 11. CNN-SVD flow chart



All elliptic curve domain parameters over $\mathbf{F}_q$ must have the form:

$$[\log_2 q] \in \{192, 224, 256, 384, 521\} \quad (14)$$

The following Tables 1-3 demonstrate a selection of some of these recommended parameters [4]:

PROTECTION OF DATA USING PRETRAINED CONVOLUTIONAL NEURAL NETWORK (CNN) AND SINGULAR VALUE DECOMPOSITION (SVD)

As proposed by is proposed by (Al-Shibli, Marques, & Spiridon, Nov. 2018), in this section Pretrained convolutional neural network (CNN) training to be implemented a part of the block chain to protect personal data and information as third wall defense against hacking. CCN is used to extract learned image features and use those features to train an image classifier with single pass making advantage of machine learning tools features as shown in Figure 11. Images can be automatically loaded from image library and labeled based on the image folder name even if images do not fit in memory. Partial training of the image data can be performed in order to test the rest image data. Pre-trained CNN can classify images into object categories.

The Pre-trained CNN architecture is composed of some convolutional layers and some fully connected layers where the first layer is dedicated as an image input layer with given size and color channels. The CNN builds a hierarchical structure of input images, meanwhile the deeper layers contain higher-level features made based on the lower-level features of previous layers. A part of the training is to extract the image labels from the training data and test data and then these features extracted from the training images are used as predictor variables and fit with a multiclass support vector machine learning (MSVML) as shown in Figure 11. Therefore, the test images can be classified and labeled. The fraction of labels that the network predicts correctly represents the accuracy.

Figure 12. Sample 1 of the pre-trained images of the CNN

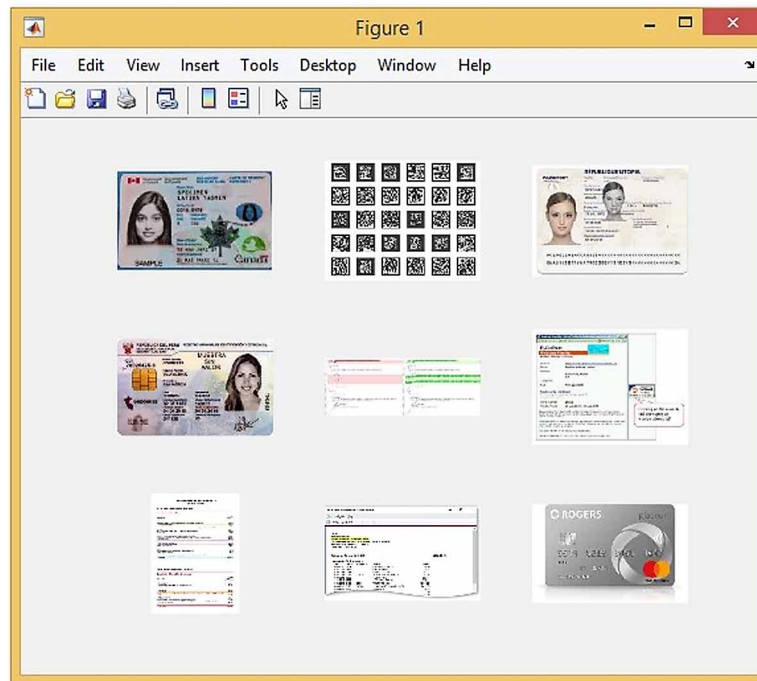


Figure 13. Sample 2 of the pre-trained images of the CNN

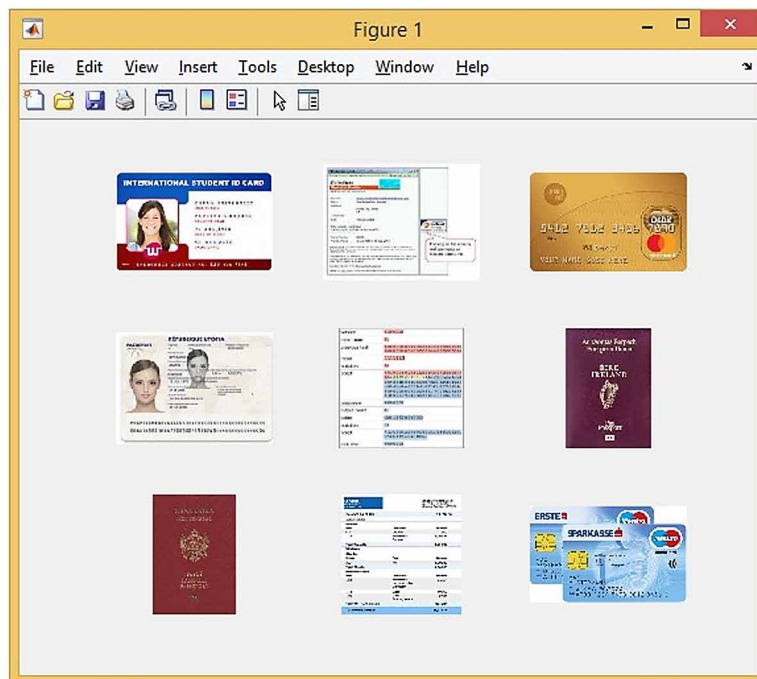


Figure 14. Sample 1 display of CNN test images with predicted labels

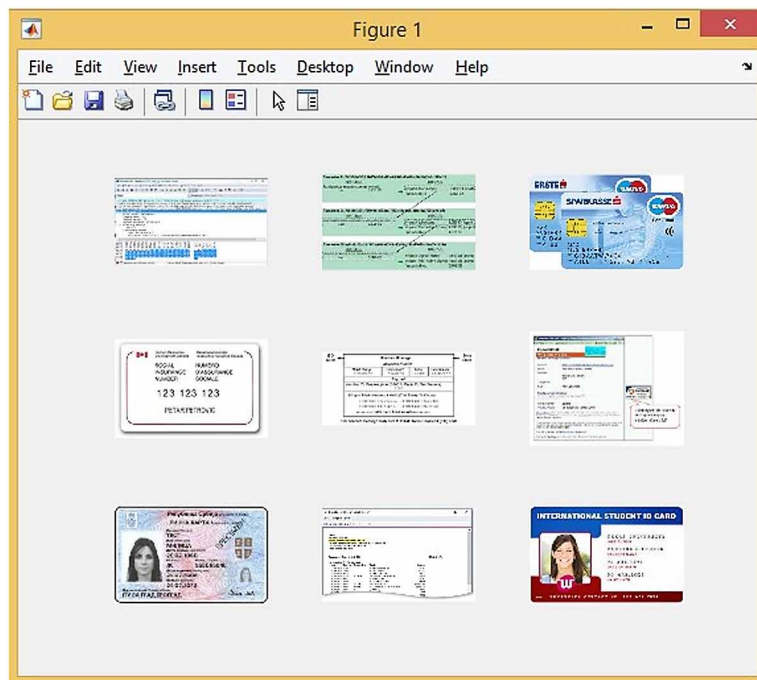


Figure 15. Sample 2 display of CNN test images with predicted labels

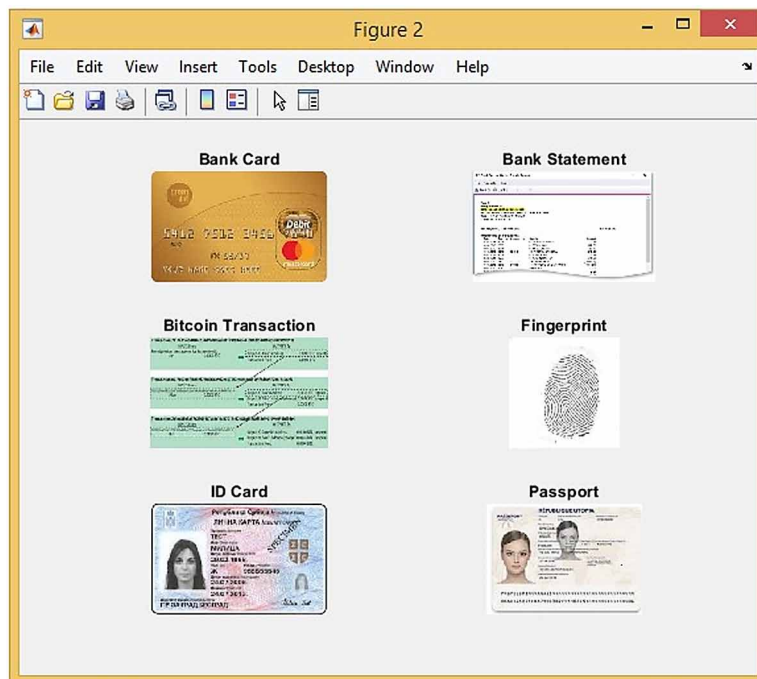
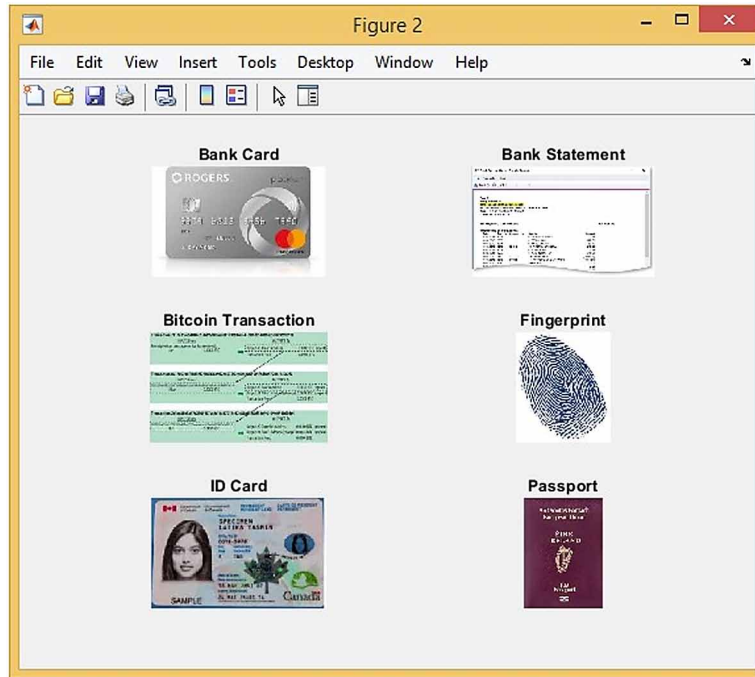


Figure 16. Block diagram of the encryption

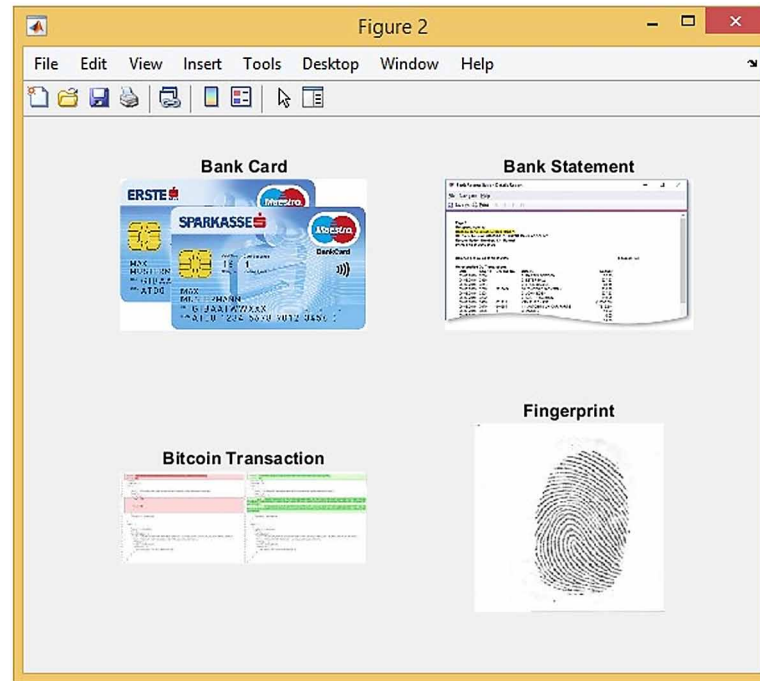


CNN-SVD Criteria

- Step 1:** Load the target images from the image library store.
- Step 2:** Divide the image data into 60% training data and 40% test data.
- Step 3:** Exhibit some of image samples.
- Step 4:** Load a pre-trained CNN network.
- Step 5:** Display the CNN architecture.
- Step 6:** Identify the size of the input images and create augmented image data-storage.
- Step 7:** Extract the class labels from the training data and test data.
- Step 8:** Classify fit image by using support vector machine learning (SVML).
- Step 9:** Classify the test images using SVML model.
- Step 10:** Display sample test images with their corresponding predicted labels.
- Step 11:** Calculate image classification accuracy.

For the purpose of demonstration of pre-trained CNN blockchain based information and image processing and classification, sample images are used to represent 6 different categories: fingerprints, ID cards, passports, bank cards, bank statements, and bitcoin transactions. These sample images are unzipped and loaded as an image data-store. Image Data store automatically labels the images based on folder names and stores the data as an Image data-store object. A total of 30 images Split the data into 70% for training and 30% for test data. In overall, there are now 21 training images and 9 validation images in this very small data set. Three runs of some of these sample images are demonstrated in Figures 12-13. Meanwhile, the CNN labeling identification are depicted in Figures 14-15 with 100% accuracy.

Figure 17. Display of SIN card image which is encrypted by using SVD



In cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing the photography, usually referred to as a key. The result of the process is encrypted information. The reverse process is referred to as decryption as shown in Figure 16. Cryptography involves the use of advanced mathematical procedures during encryption and decryption processes. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric. Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of image matrix and decryption of cipher image matrix. The keys may be identical or there may be a simple transformation to go between the two keys.

The proposed encrypt image based on SVD can be applied the colored images into grayscale images Al-Shibli (Oct. 2015). The encryption technique includes the SVD transformation of the resulted grayscale image; converting decimal numbers to binary numbers of the SVD matrix; converting decimal numbers to binary numbers of random vector as the first cipher key; running logical Exclusive OR as a second cipher key; adding noise to the image by using Poisson distribution as a third cipher key; implementing another stage of decimal-to-binary and logical Exclusive OR; running binary-to-decimal conversions; and finally obtaining the encrypted SVD matrix. The following 17 steps outline the encryption criteria in details along with testing results in Figures 16-17:

- Step 1:** Read image from graphics file.
- Step 2:** Convert RGB image or colored map to grayscale.
- Step 3:** Convert image to double precision.
- Step 4:** Display image in Handle Graphics figure.
- Step 5:** Convert image into SVD.

Figure 18. Display of encrypted SVD images of sin card image shown in figure 17

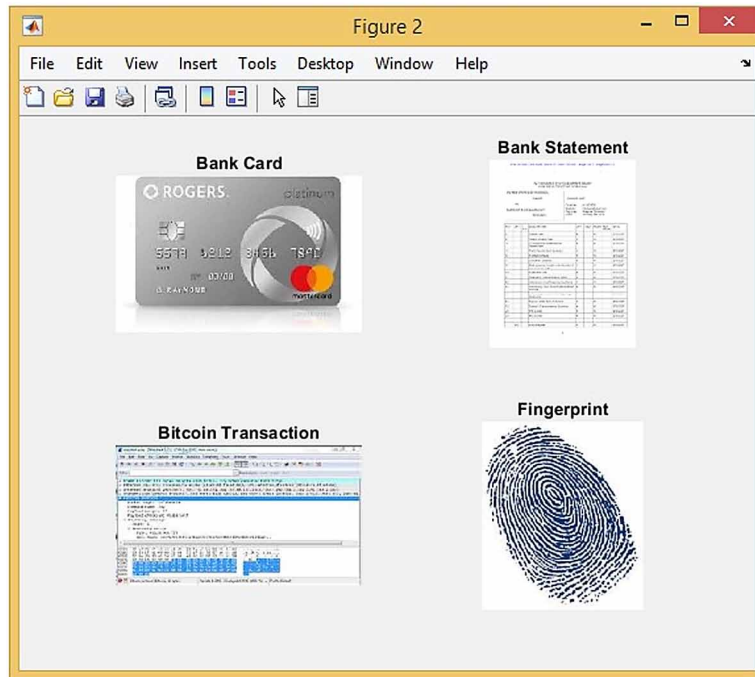
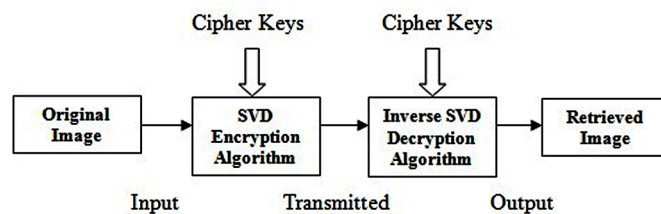


Figure 19. Display of reconstructed SIN card image by decryption of SVD images



Step 6: Return a vector containing the singular values of SVD.

Step 7: Round towards nearest integer.

Step 8: Convert decimal numbers of the vector to binary numbers.

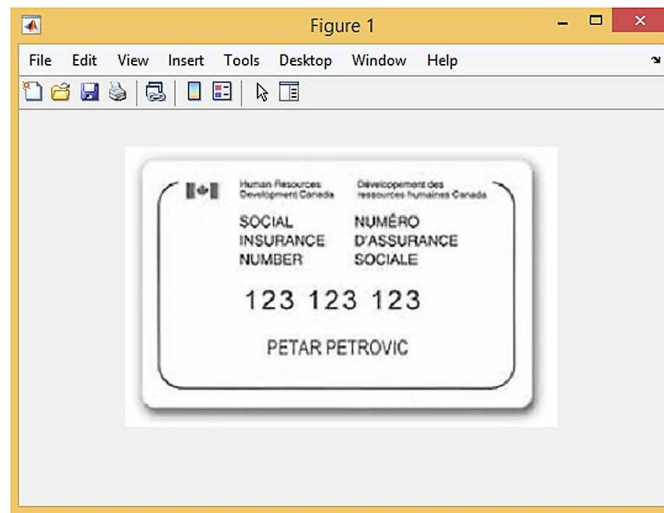
Step 9: Convert decimal numbers of a random vector to binary numbers.

Step 10: Run Logical EXCLUSIVE OR of Step 8 and Step 9 to obtain the logical symmetric difference of elements of both vectors. $XOR(S,T)$ is the logical symmetric difference of elements S and T . The result is logical 1 (TRUE) where either S or T , but not both, is nonzero. The result is logical 0 (FALSE) where S and T are both zero or nonzero. S and T must have the same dimensions (or one can be a scalar).

Step 11: Generate random arrays from a specified Poisson distribution (Adding noise to the image).
 $R = \text{Random}(\text{Poisson}, A)$: Returns an array of random numbers chosen from the one-parameter probability Poisson distribution with parameter values A .

Step 12: Convert decimal numbers of the vector to binary numbers.

Figure 20. Pretrained CNN encryption-decryption identification of the blockchain information



Step 13: Run Logical EXCLUSIVE OR of Step 10 and Step 12.

Step 14: Convert decimal numbers of the vector to binary numbers.

Step 15: Convert to diagonal matrix. $\text{DIAG}(V, K)$ when V is a vector with N components is a square matrix of order $N + \text{ABS}(K)$ with the elements of V on the K -th diagonal.

Step 16: Convert to SVD using the diagonal matrix obtained in Step 15.

Step 17: Convert to encrypted image

In order to verify that the proposed technique is effective, SVD encryption-decryption of a SIN card image set has been implemented as depicted in Figure 17. This image is encrypted in three images as shown in Figure 18. For the purpose of validation, the SVD image matrices are then decrypted to recover and reconstruct the original SIN image which is successfully achieved in Figure 19.

The decryption process is the inverse process of encryption; the algorithm implements a logical Exclusive OR, decimal to binary conversion and then SVD transformation. Detailed algorithm of the decryption process with 7 steps is as follows:

Step 1: Run Logical EXCLUSIVE OR of Step 13 and Step 12 in Section IV.

Step 2: Run Logical EXCLUSIVE OR of Step 10 and Step 9 in Section IV.

Step 3: Convert decimal numbers of the vector to binary numbers.

Step 4: Convert to diagonal matrix.

Step 5: Convert to SVD using the diagonal matrix obtained in Step 4 in this current section.

Step 6: Convert to decrypted image.

Step 7: Display decrypted image with predicted label.

Furthermore to the analysis, Figure 20 demonstrate that the CNN encryption-decryption technique is crucially efficient in processing the drone image set. Initially, (1) pretrained CNN image training and testing steps are performed as start; then (2) the 17 SVD encryption steps are followed to generate an unreadable images; finally, (3) the decryption algorithm introduced earlier is used to recover the original images as demonstrated in Figures 12-18. In all runs, the pretrained CNN network is loaded as an input

to train this set of images. AlexNet network is used as a tool in this analysis. This network is used to train and classify images. This network is composed of 5 convolutional layers and 3 fully connected layers such that the first layer is used as the image input layer. Deeper layers contain higher-level features, constructed using the lower-level features of earlier layers. In order to get the feature representations of the training and test images the fully connected layer are activated. Meanwhile, lower-level representation of the images, earlier layers are used. Based on the training and test data, labels then are successfully extracted.

CONCLUSION

In this chapter an overview of multilayer neural networks and associated application to blockchain and bitcoin technology is presented along with prospective and future applications. Recently blockchain has been received special attention due to its encrypted data and secure digital of peer-to-peer transactions. It is noticed that blockchain has a strong potential to be used as a digital platform to process and store digital information and transactions using special secure cryptology techniques based on the elliptic curves digital signature algorithm (ECDSA). It is reported that this technology is worth \$630 billion a year industry with an annual growth of 7%. The implementation of blockchain has a promising future represented in saving million working hours per annum, saving more million printed documents annually, saving around billion dollars in transactions and ensuring the digital security of national and international documents and transactions.

Therefore, blockchain is a promising ledger which can be used as a new platform for digital information and to store encrypted data and process secure digital transactions. This blockchain possess strong features that enable users to store sensitive personal data and financial credentials. But it happened that many reports that claim bitcoin wallets have hacked and led into losing investments. Therefore, this chapter proposed a multi-layer encryption technique along with artificial intelligent neural networks codes to be implemented to enhance the encrypted data and security characteristics. In particular, AINN Machine learning can be very effective in hashing algorithms of mining transactions blocks of Bitcoin blockchain platform compared to a tedious time consuming tradition approach. In order to protect personal data and information as third wall defense against hacking, the utilization of pretrained convolutional neural network (CNN) is proposed to be a part of the block chain. CCN is used to extract learned image features and use those features to train an image classifier with single pass making advantage of machine learning tools features. Simulation results demonstrates the effectiveness of using pre-trained CNN blockchain-based information. In particular processing and classification of document and images of 6 different categories are 100% efficient to classify fingerprints, ID cards, passports, bank cards, bank statements, and bitcoin transactions.

This new innovative technology has its own advantages and disadvantages that receives some supports as well as some concerns. Advantages of the Blockchain Technology:

- Zero Percentage of Fraud;
- Non-centralized Process;
- Instant Transactions;
- Improved Financial Efficiency.

Disadvantages of the Blockchain Technology:

- Digital black market;
- Non-Tangible and Extremely Volatile;
- High Tech for Traditional Customers or Operations.

In overall, this chapter introduces a novel integrated cryptology approach of artificial intelligence based blockchain by introducing a multilayer security layer and neural networks machine learning techniques. Specifically, this revolutionary safe combination criteria is structured by implementing a coupled private key elliptic curves digital signature in order to securely enter into the blockchain and process encrypted data using neural networks. By the virtue of this algorithm and by using blockchain and AI network service will provide users, owners and organizations with security measures needed to ensure that their data is safe from attacks and siphoning. Moreover, this will provide business enterprises with blockchain technology to prevent any attempts by hackers to conduct cyber-attacks.

REFERENCES

- Al-Shibli, M. (2015). UAS Image Encryption-Decryption Using Singular Value Decomposition (SVD) and Random-Poisson-XOR-Keys Techniques. *World Congress on Unmanned Systems Engineering*, Granada, Spain. 10.14323/ijuseng.2015.17
- Al-Shibli, M. (2019). *Blockchain-Enabled Peer-to-Peer Drone Delivery Service*, EFS ID: 34727686, Application Number 62786800. USPTO Patent.
- Al-Shibli, M. (2019). *Blockchain Artificial Intelligent Drone Network and Cloud System*, EFS ID: 34731423, Application Number 62787335. USPTO Patent.
- Al-Shibli, M. (2019). *Blockchain Drone Satellite Network System (BlockchainDroneSatNet) and Cryptocurrency (Drone Satellite Coin: DSAC AND Drone Satellite Token: DSAT)*, EFS ID: 34737619, Application Number 62787531. USPTO Patent.
- Al-Shibli, M. (2015, Oct.). Dynamic UAS Image Encryption-Decryption Using Singular Value Decomposition (SVD) and Random-Poisson-XOR-Keys Techniques. *International Journal of Unmanned Systems Engineering*.
- Al-Shibli, M., Marques, P., & Spiridon, E. (2018). Artificial Intelligent Drone-Based Encrypted Machine Learning of Image Extraction Using Pretrained Convolutional Neural Network (CNN), Big Data and Machine Learning (BDML) 2018. ACM.
- American National Standards Institute (2001). *Public-Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*. American National Standard X9.63.
- American National Standards Institute (2005). *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standard X9.62.
- Besarabov, Z. & Kolev, T. (2018). *Predicting digital asset market based on blockchain activity data*. International Science and Engineering Fair.
- Bi, W, Jia, X., Zheng, M. (2018). *A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain, Computer Science, Cryptography and Security*. arXiv.org.

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014). Elliptic Curve Cryptography in Practice, Financial Cryptography and Data Security. *18th International Conference, Revised Selected Papers, FC 2014*, Christ Church, Barbados.

Brown, D. R. L. (2009). *Standards for Efficient Cryptography Group. SEC 1: Elliptic Curve Cryptography*. Certicom Corp. Research, Version 2.0.

Brown, D. R. L. (2010). *SEC 2: Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography*. Certicom Corp. Research, Version 2.0.

Crossen, S. (2015). *The Mathematics of Bitcoin* (Master Thesis). Department of Mathematics Emporia State University.

Ghosh, A. & Nath, A. (2014). Cryptography Algorithms using Artificial Neural Network. *International Journal of Advance Research in Computer Science and Management Studies*, 2(11).

Giechaskiel, I., Cremers, C., & Rasmussen, K. B. (Feb. 2016). On Bitcoin Security in the Presence of Broken Crypto Primitives. *European Symposium on Research in Computer Security (ESORICS 2016)*, 201-222. 10.1007/978-3-319-45741-3_11

Haddaji, R., Ouni, R., Bouaziz, S., & Mtibaa, A. (2016). Comparison of Digital Signature Algorithm and Authentication Schemes for H.264 Compressed Video. *International Journal of Advanced Computer Science and Applications*, 7(9), 2016. doi:10.14569/IJACSA.2016.070949

Khalique, A, Singh, K., & Sood, S. (2010). Implementation of Elliptic Curve Digital Signature Algorithm. *International Journal of Computer Applications*, 2.

Kheradmand, B. (2013). Enhancing Energy Efficiency in Wireless Sensor Networks via Improving Elliptic Curve Digital Signature Algorithm. *World Applied Sciences Journal*, 21(11), 1616–1620.

Kikwai, B. K. (2017). Elliptic Curve Digital Signatures and Their Application in the Bitcoin Cryptocurrency Transactions. *International Journal of Scientific and Research Publications*, 7(11).

Kolhekar, M., & Jadhav, A. (2011). Implementation of Elliptic Curve Cryptology on Text and Images. *International Journal of Enterprise Computing and Business Systems*, 1(2).

Linke, B. (2014). *The Fundamentals of an ECDSA Authentication System*. Tutorial Article, Maxim Integrated.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Academic Press.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.

Wireless Application Forum. (2001). *Wireless Transport Layer Security*. Wireless Application Protocol WAP-261-WTLS-20010406-a, Version 06.

ADDITIONAL READING

- Saifedean, A. (2018). *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley.
- Venkatesan, R., & Li, B. (2017). *Convolutional Neural Networks in Visual Computing: A Concise Guide*. CRC Press. doi:10.4324/9781315154282

KEY TERMS AND DEFINITIONS

Bitcoin: Invented in 2008 by Satoshi Nakamoto to create a decentralized digital currency used to record peer-to-peer transactions generated by complicated mathematical models to ensure security without the need for intermediaries such as central banks.

Blockchain: A system made-up of blocks that are used to record transactions in a peer-to-peer cryptocurrency network such as bitcoins.

Convolutional Neural Networks (CNN): A special type of neural networks used popularly to analyze photography and imagery.

Cryptology: A technique used to secure communicating of information, data and messages by implementing special protocols and algorithms aims to prevent other parties from reading and understanding the information transmitted.

Digital Signature: A secure mathematical algorithm used to validate the credentials of digital documents and coded information associated with pre-approved signer to approve transactions.

Elliptic Curves Digital Signature Algorithm (ECDSA): Is a mathematical cryptology technique used by digital currencies and Bitcoin to ensure the security of the peer-to-peer transactions using secret codes and keys.

Encryption-Decryption: An algorithm used to transform information to something random, meaningless and not readable, and then translate it back to something understandable.

Singular Value Decomposition (SVD): A factorization mathematical algorithm of matrices used in diverse application such as signal processing, communication, and imagery.

An IBE–Based Authenticated Key Transfer Protocol on Elliptic Curves

Daya Sagar Gupta

 <https://orcid.org/0000-0001-5401-7287>

Sher Shah College of Engineering Sasaram Bihar, India

INTRODUCTION

The twentieth century grew with the rapid development in the area of Internet and Mobile Communications Technologies/Applications, called Information and Communication Technology (ICT). ICT services have grown exponentially and become beneficial to the world in different ways. However, these technologies are changing very frequently, and several services with multimedia applications are growing through various real-life applications. In these regards, the security protection to various services becomes essential and challenging as well, and different security mechanism for different encryption, authentication, and integrity easy data availability technologies are being developed in a rapid pace. In order to design different security mechanisms and meet the challenges, different cryptographic primitives are used in their convenient ways. In the era of Internet technology; key transfer protocols are playing a crucial role in the network and information security field. These protocols are mainly incorporated to transfer a common session key among different user. The key exchanged using these protocols is generally used for symmetric key encryption where this key is known as private key and used for both encryption as well as decryption. As we all know, many key transfer protocols including basic Diffie-Hellman protocol, are proposed in the literature. However, many of these key transfer protocols either are proven insecure or had a burden of communication and computational cost. Therefore, a more secure and efficient key transfer protocol is needed. In this paper, the author proposes an authenticated key transfer protocol, which securely and efficiently negotiates a common session key between two end users. He calls this protocol as IBE-TP-AKE. This proposal is based on the elliptic-curve cryptography (ECC) and uses the idea of identity-based encryption (IBE) with pairing. The security of the proposed work is based on the hard problems of elliptic curve and their pairing extensions discussed in Gupta & Biswas (2015a), Gupta & Biswas (2015c) etc. Further, the author has shown the security of his proposed protocol and proved it using the security properties discussed later. All security properties of key exchange protocol is possessed by our proposed protocol. As we know, cryptography is a branch of science and it is an art to use security primitives in a way to deal with the security challenges and meet the solutions. Data encryption in cryptography is divided into two major categories namely, symmetric/private-key and asymmetric/public-key techniques in which the latter one has greater research impact than the former. However, the useful public-key cryptographic techniques like RSA, ElGamal etc. have some disadvantage as they require extensive public key management overheads. Thus, new technique called, identity-based encryption (IBE) is introduced recently and is used by researchers to design efficient cryptographic tools for different security applications. In this article, the author has formulated the idea of this technique to implement his protocol. Shamir (1984) has firstly proposed the novel idea of IBE by choosing the known identity of a user as public-key. This known identity may be Email, Ph. No, IP address etc. Using the

DOI: 10.4018/978-1-5225-9715-5.ch076

identity of a user as public-key, Shamir removed the overhead of certificate management from public-key cryptography. In addition, a trusted third party Private Key Generator (PKG) is considered to generate user's private key. However, the practical implementation of IBE is considered in Boneh & Franklin (2001). This proposed IBE-TP-AKE protocol includes the properties of a pairing technique as defined in Gupta & Biswas (2015b). This bilinear map relates two members of a group to a member of another group. For this particular paper, a bilinear mapping technique takes two members (points) of an elliptic curve group and maps it to a member of another multiplicative group. However, authentication to our proposed IBE-TP-AKE scheme is provided by means of the ECC. The elliptic curve hard assumptions are the hard problems which are used to efficiently secure the presented protocol. The security provided by the ECC is efficient than that of RSA. A 160-bit key in ECC provides the same level of security provided by a 1024-bit key size in RSA as Gupta & Biswas (2017). The points of the elliptic curve group generate an abelian group which is used to generate the cryptographic algorithms.

BACKGROUND

Diffie and Hellman (1976) were the first who gave a new idea of having two separate keys; one for encipherment and other for decipherment. This proposal gave the birth to the key exchange protocol which is named as Diffie and Hellman (DH) key exchange protocol. Their idea was to exchange a common secret key between two authentic entities. But unfortunately, their proposal is vulnerable to a number of attacks which includes well known man-in-the-middle (MITM) attack. To eliminate these difficulties, research has grown in this direction and many researchers have proposed different type of key transfer protocols like Liu et al. (2012), Gupta & Biswas (2016), Gupta & Biswas (2017a), Cheng et al. (2013), Gupta et al. (2018a) etc. Jeong et al. (2004) designed many two party key agreement protocols which are executed in one round of communication. They claim that the proposed protocols are authenticated and resist many attacks. McCullagh & Barreto (2005) proposed a key agreement protocol for two parties which were developed in IBE framework. They showed that their protocol is efficient and secure than other existed state-of-the-arts. They also presented the comparative analysis for their proposed key agreement scheme. Choo (2005) reviewed McCullagh & Barreto (2005) and showed that their protocols are vulnerable if the attacker has sent the *Reveal* query. Hölbl et al. (2012) devised an identity-based key exchange scheme for two parties. For their proposal, they used the pairing technique and also derived a variant of signature schemes which confirms the security of their proposal. They also claimed that their protocol is comparatively secure and cost efficient. Gupta & Biswas (2017b) proposed two secure bi-partite key agreement protocols using the IBE and pairing. The first protocol is based on the DH key agreement protocol; however the later is based on the elliptic curve group. They further extended their two party key exchange protocol for three party key exchange protocols. They showed that their protocols are secure against many attacks and claimed that these protocols exhibit better security and efficiency than other similar literatures. Tseng (2007) proposed an identity based key agreement protocol based on the hard problem of discrete logarithm. It was claimed that the computation and communication cost of his protocol is better than other competing protocols. His protocol is secure and resistance to many possible attacks. Gupta & Biswas (2018b) devised two authenticated key exchange protocol using signature and signcryption authenticators. The security of their protocols is based on the lattice hard problems. They claimed that their protocols resist the quantum attack.

TECHNICAL TERMS AND DEFINITIONS

Moreover, the definitions and notations used in the development of this paper is considered and explained below:

Elliptic Curve Cryptography (ECC): Miller (1985) firstly introduced the concept of an elliptic curve cryptosystem. By using ECC, he designed a key agreement protocol which is similar to DH key agreement protocol. Later, Koblitz (1987) also proposed a cryptosystem based on the elliptic curve. A cryptographic elliptic curve of prime order p is denoted by E/F_p and is expressed as the following equation:

$$y^2 = x^3 + ax + b$$

In the above equation, a and b are the elements of F_p and satisfies the relation $4a^3 + 27b^2 \neq 0$. All the points of elliptic curve forms an additive group with commutative operation. This “+” operation on points is defined as follows:

Let the two point of an additive group E/F_p be L and T . The addition of points L and T can be calculated as following conditions:

- Let these two points L and T are different point on the curve having different x and y coordinates and the line joining these two points cuts the curve on another point $-Y$, then the image of $-Y$ about x -axis gives the addition $L+T$ i.e. $Y=L+T$. Here, the points Y and $-Y$ are known to inverse to each other with respect to elliptic curves.
- Let these two points L and T overlaps i.e. $L=T$. In this case, the line joining these same points will be the tangent to the curve and let it cuts the curve on a point $-Y$, then the image of $-Y$ about x -axis gives the addition $L+T$ i.e. $Y=L+L=2L$ or $2T$.
- Let two points to be added are inverse to each other i.e. the points on the curve are L and $-L$, thus the line joining these points cuts the elliptic curve at Infinity called point of Infinity and denoted by O . Thus the addition is $L + (-L) = O$. The point of infinity is the identity of elliptic curve.
- The scalar multiplication on the elliptic curve can be calculated by adding the same point scalar times i.e. kL can be calculated by adding L using the above rules, k time.

Bilinear Mapping: The technique of bilinear mapping is mainly used in the IBE to pair two groups of same order. In recent years, bilinear pairing has played an essential role in designing many cryptographic primitives. Let there are two groups namely G_1 and G_2 both having the same order q where q belongs to a number from prime set. The group G_1 is considered as an elliptic curve group, whereas group G_2 is a multiplicative group of same order. A bilinear mapping is denoted by $\hat{e}: G_1 \times G_1 \rightarrow G_2$ which maps two elements of G_1 to an element in G_2 and defined by these three properties:

- **Bilinearity:** This property executes $\hat{e}(lL, tT) = \hat{e}(L, T)^{lt}$ for all $L, T \in G_1$ and $l, t \in \mathbb{Z}_q^*$.
- **Non-Degeneracy:** This property tells that the mapping does not map all pairs in $G_1 \times G_1$ to the identity element in G_2 .
- **Computability:** The bilinear mapping $\hat{e}(L, T)$ can be efficiently computed for $L, T \in G_1$.

Further, it can be easily seen that the bilinear operation exhibits the commutative property i.e. $\hat{e}(L, T) = \hat{e}(T, L)$.

Identity-based Encryption: The public-key encryption (PKE) scheme involves a lot of overhead in the certificate management. Further, a public-key certificate is also need to be verified by the user for the validation of the public key. To eliminate the overhead of certificate management in the classical PKE, as early as 1984, Shamir (1984) firstly gave an idea about a PKE scheme where an identity of the user is treated as the public-key and it is named as Identity-based Encryption (IBE). This was the original motivation for IBE. In IBE, the public-key can be any arbitrary string and a sender may use an identity (say ID) of the receiver for encryption of the messages. For instance, when Alice sends a message to Bob, she encrypts her message using the Bob's public identity as email address "bob@ domainname. com". Then, Bob can decrypt the message using a private key taken securely from private key generator (PKG) through proper authentication. This novel concept of Shamir's proposal initiates a paradigm shift in public-key cryptographic techniques. However, until the year 2001, it was an open challenge for the researchers to construct a fully functional and efficient IBE. Boneh & Franklin (2001) firstly proposed a fully functional IBE from the Weil Pairing. The IBE scheme mainly depends on a trusted authority, called PKG who generates the global system parameter *param* and the secret key for the users according to their public identity. IBE comprises four randomized algorithms namely, *setup*, *extract*, *encrypt* and *decrypt*. The generated private-key is transferred to the data user via a secure channel. With the nice functionality that any party can perform the encryptions of messages with no prior keys distribution among individual parties, IBE gains lots of attention from industry, research and academic community. The four algorithms of IBE are as follows:

- **Setup:** This algorithm is used to generate the system parameters *param* and executed by a third party PKG. The input to Setup algorithm is a security parameter *t* and the output is generated *param* including the master secret of PKG.
- **Extract:** This algorithm is used for key extraction and also executed by PKG. The input to Extract algorithm is the identity ID of a user and the output is private key of the user. The PKG securely transmits private key to its owner.
- **Encrypt:** This algorithm is run by the sender of a message *m*. The input to Encrypt algorithm is a message *m* and the output is the encrypted message, called cipher text generated using the *param*.
- **Decrypt:** This algorithm is run by the receiver for decryption of the cipher text. The input to Decrypt algorithm is cipher text and output is plain text message recovered using the private key of receiver.

Security properties: The security properties of any key agreement protocols must be protected from an adversary. An adversary can attack on the key exchange protocol in many ways to breach its security. Thus, the development of key exchange protocols should be done in very careful manner so that the designed key must resist all the possible types of attack. For designing a secure key, some security properties must be defined as described in the Bellare & Rogaway (1993). Let P_1 and P_2 be two authentic users. The following security properties must be possessed by the proposed IBE-TP-AKE protocol:

- **Man-in-the-Middle (MITM) Attack:** This attack is very well known attack. An attacker impersonates both the authentic entities to exchange two different keys with them. One key is used with a user and another is used another user.
- **Known Key Security:** This security confirms that if session keys which are negotiated in previous rounds are compromised to the adversary then the current round key must not be compromised i.e. the session keys which are executed in the current round should be independent to other rounds keys.

- **Key Control:** Any authentic user can not be able to generate the session key individually. To generate the correct session secret key, the involvement of both the users is compulsory.
- **Unknown Key-Share Resilience:** In this security, it is believed that a user P_1 is not negotiating a session key with a third party called, adversary instead of P_2 while P_2 believes that the key is shared with him and P_1 .
- **Perfect Forward Secrecy:** In this security, it is believed that if private keys of any or all users are known to the adversary, then the adversary cannot get the previously generated session keys with the help of these private keys.
- **Key-Compromise Impersonation Resilience:** In this security, it is desired that if the private key of a user say P_1 is compromised by the adversary, then the adversary cannot impersonate the other user P_2 . It is obvious that adversary can impersonate P_1 easily because he knows the private key.

Computational Problems: Some computational hard assumptions are laid here:

- **Discrete Logarithm Problem (DLP):** This hard problem states that if a and b are taken from a multiplicative group i.e. $a, b \in G_2$ and a and b are known where $b = a^r \mod q$ for all $r \in \mathbb{Z}_q^*$, then it is hard to find the value of r .
- **Elliptic Curve Discrete Logarithm Problem (ECDLP):** This hard problem states that if L and T are taken from an additive group i.e. $L, T \in G_1$ and L and T are known where $T = rL$ for all $r \in \mathbb{Z}_q^*$, then it is hard to find the value of r .
- **Bilinear Diffie-Hellman Problem (BDHP):** This hard problem states that if L is taken from an additive group i.e. $L \in G_1$ and L, xL, yL and zL are known where $x, y, z \in \mathbb{Z}_q^*$, then it is hard to find $\hat{e}(L, L)^{xyz}$.
- **Computational Diffie-Hellman problem (CDHP):** This hard problem states that if L is taken from an additive group i.e. $L \in G_1$ and L, xL and yL are known where $x, y \in \mathbb{Z}_q^*$, then it is hard to find xyL .

PROPOSED IBE-TP-AKE PROTOCOL

In this section, the designed IBE-TP-AKE protocol is laid down. This proposed protocol is developed using IBE framework. In this protocol, security of negotiated key and authentication of users are ensured using the different hard assumptions as discussed earlier. However, the computational as well as communication complexities are also reasonable. Suppose the sender S wants to negotiate a common secret key with the receiver R . Except the sender and receiver, a third entity PKG is also involved in the protocol. The phases of proposed IBE-TP-AKE protocol are described as following steps:

1. **Initialization Phase:** The initialization phase of the proposed protocol consists of following algorithms as IBE discussed earlier:
 - a. **Setup:** This algorithm of the proposed IBE-TP-AKE protocol is executed by PKG and it take a security parameter t as input and generates the following parameters:
 - i. A t -bit prime number q and two q order groups G_1 and G_2 in which group G_1 is considered as an additive elliptic curve group, whereas group G_2 is a multiplicative group of same order.
 - ii. A bilinear pairing $\hat{e}: G_1 \times G_1 \rightarrow G_2$.

- iii. A primitive element P in G_1 and a generator g in G_2 .
- iv. Two hash functions (cryptographic) H_1 and H_2 defined as $H_1: \{0, 1\}^* \rightarrow G_1$ and $H_2: G_2 \rightarrow \{0, 1\}^q$.
- v. A master secret s which is secret to the PKG and master public key $P_{pk} = sP$.

PKG publically announces system parameters $param = \{q, H_1, H_2, G_1, G_2, P, \hat{e}, P_{pk}\}$ and kept master secret as private to itself.

- b. **Key Extraction:** This algorithm of the proposed IBE-TP-AKE protocol is also executed by PKG to extract the private key of users S and R . The PKG executes these steps:
 - i. The users request the PKG with their identities ID_i for $\{i=S, R\}$.
 - ii. PKG checks the authenticity of the users S and R and calculates their private keys as P_{pri} as $P_{pri} = sQ_i$ for $\{i=S, R\}$. Here, $Q_i = H_1(ID_i)$.
 - iii. The public keys of the users are Q_i . It may be noticed that there is no need of public key certificates to verify the public key of users.
- 2. **Key Exchange Phase:** In this phase, the users S and R negotiate a common secret key between them. Let, S is the initiator and R is the responder of the proposed IBE-TP-AKE protocol. The steps used to exchange the secret key are as follows:
 - c. User P_1 initiates the protocol and does the followings:
 - i. Selects a random integer $a \in Z^*$. P_1 then computes the key related message as $u = g^a \mod q$.
 - ii. Calculates $\mu_s = \hat{e}(P_{pri_s}, X_s)$ using his private key P_{pri_s} where $X_s = aP$.
 - iii. Computes $\sigma_s = u \oplus H_2(\mu_s)$ and sends $Y_s = aQ_s$, u and σ_s to P_2 .
 - d. After receiving the messages, user P_2 responds in the following manner:
 - i. Computes $\gamma_r = H_2(\hat{e}(Y_s, P_{pk}))$ and checks $u = ? \sigma_s \oplus \gamma_r$. If the verification is true then P_2 picks a random integer $b \in Z^*$ and computes common secret key K_2 as $u^b \mod q$. Thus, the computed key $K_2 = g^{ab} \mod q$.
 - ii. Computes the key related message $v = g^b \mod q$.
 - iii. Calculates $\mu_r = \hat{e}(P_{pri_r}, X_r)$ using his private key P_{pri_r} where $X_r = bP$.
 - iv. Computes $\sigma_r = v \oplus H_2(\mu_r)$ and sends $Y_r = bQ_r$, v and σ_r to P_1 .
 - e. Finally after receiving the messages, P_1 computes $\gamma_s = H_2(\hat{e}(Y_r, P_{pk}))$ and checks $v = ? \sigma_r \oplus \gamma_s$. If the verification is true then computes common secret key K_1 as $v^a \mod q$. Thus, the computed key $K_1 = g^{ab} \mod q$.

Thus, it may be easily seen that $K_1 = K_2 = g^{ab} \mod q$. Note that the proposed protocol executes in only one round of communication and the proof of the verification $v = ? \sigma_r \oplus \gamma_s$ (and the proof of $u = ? \sigma_s \oplus \gamma_r$ is similar) is given below.

Since

$$\begin{aligned}
 \sigma_r \oplus \gamma_s &= v \oplus H_2(\mu_r) \oplus \gamma_s \\
 &= v \oplus H_2(\hat{e}(P_{pr}, X_r)) \oplus H_2(\hat{e}(Y_r, P_{pk})) \\
 &= v \oplus H_2(\hat{e}(sQ_r, bP)) \oplus H_2(\hat{e}(bQ_r, sP)) \\
 &= v \oplus H_2(\hat{e}(Q_r, P)^{bs}) \oplus H_2(\hat{e}(Q_r, P)^{bs})
 \end{aligned}$$

= v (Proved)

SECURITY ANALYSIS OF PROPOSED IBE-TP-AKE PROTOCOL

This section comes with the security analysis of our proposed IBE-TP-AKE protocol. Our presented protocol resists all possible security attacks which can be used to breach the security of a key exchange protocol. The different type of security attacks are discussed below and it has been proved that our proposed IBE-TP-AKE protocol is secure against all these type of attacks.

1. **Man-in-the-Middle (MITM) Attack:** Our proposed IBE-TP-AKE protocol negotiates a common secret key and security of this key is provided using the signature σ_i for $i = s, r$ of individual users. In our protocol, users S and R generates the signatures σ_s and σ_r using their private keys respectively. If an adversary $\hat{A}$ tries to impersonate any of the authentic users S and R, she cannot generate a valid signature and thus it is difficult for $\hat{A}$ to impersonate S and R. Hence, our IBE-TP-AKE protocol is not vulnerable to MITM attack.
2. **Known Key Security (K-KS):** In our protocol, the negotiated secret key K in each session is unique because the secret key K is generated using the ephemeral secret values a and b chosen by users S and R at random. Thus, if adversary $\hat{A}$ has the access to previous session secret keys, she might not be able to derive the current or future session keys. Thus, K-KS attack is resisted by our protocol.
3. **No Key Control (NKC):** A single user in our protocol cannot derive the correct session key because both ephemerals a and b are not known to him. It is necessary for our proposed protocol that both S and R must be involved in the process of generating the session secret key. An individual user cannot enforce the correct key K. Thus, the proposed key exchange protocol is free from NKC attack.
4. **Unknown Key-Share (UK-S) Resilience:** The proposed protocol requires the private keys P_{pri} and identities ID_i for $i = s, r$ of users S and R to generate the signature σ_i . Adversary $\hat{A}$ cannot generate the valid signature σ_i which can be verified by the authentic parties S and R. Thus, it is not possible by a user either S or R to share a correct key with $\hat{A}$. Hence, our proposed protocol resists UK-S attack.
5. **Perfect Forward Secrecy (PKS):** The adversary $\hat{A}$ cannot recover the previous session keys even after getting the private keys P_{pri} for $i = s, r$ of all authentic users S and R because in the process of key generation the ephemeral secrets a and b which are chosen at random by S and R. It is difficult for $\hat{A}$ to recover a and b from $g^a \bmod q$ and $g^b \bmod q$ respectively because of DLP. Thus, the proposed protocol follows PKS.

6. *Key-compromise impersonation (K-CI) resilience:* In this type of attack, the adversary $\hat{A}$ somehow get the private key of one user, say P_{prs} of user S . Now, $\hat{A}$ tries to impersonate R to S but she is not able to do so because she do not know the private key $P_{pr\hat{r}}$ of another user R . Thus, K-CI attack is prevented by out IBE-TP-AKE protocol.

FUTURE RESEARCH DIRECTIONS

The key exchange protocols play a vital role in design of cryptographic protocols either symmetric or asymmetric. This chapter executed a key exchange protocol which is secure and efficient. However, more secure and efficient key exchange protocols are needed for the different type of lightweight applications. The authors considered these novel protocols as open problem. Further, the quantum computer may exist in future and it is believed that the classical hard assumption may be broken by the quantum computer. Thus, there is a need of key exchange protocols which can resist the quantum attack. This problem of developing quantum free key exchange protocol is also supposed to be open.

CONCLUSION

A novel and efficient authenticated key agreement protocol is devised in this chapter. The proposed key agreement protocol is executed for two users and the negotiated key is shared between both the users. For development of key exchange protocol, the author has used the concept of IBE and bilinear pairing. The security of the proposed protocol is ensured using the hard assumptions of elliptic curve as well as DLP. Further, the security of proposed IBE-TP-AKE protocol is analyzed in the view of all its security properties. The author has proved the security proofs of proposed protocol. Author has given the open problems related to key agreement schemes.

REFERENCES

- Bellare, M., & Rogaway, P. (1993, August). Entity authentication and key distribution. In *Annual international cryptology conference* (pp. 232-249). Springer.
- Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In *Annual international cryptology conference* (pp. 213-229). Springer. 10.1007/3-540-44647-8_13
- Cheng, Z. Y., Liu, Y., Chang, C. C., & Guo, C. (2013). A fault-tolerant group key agreement protocol exploiting dynamic setting. *International Journal of Communication Systems*, 26(2), 259–275. doi:10.1002/dac.2506
- Choo, K. K. R. (2005). Revisit Of McCullagh-Barreto Two-Party ID-Based Authenticated Key Agreement Protocols. *International Journal of Network Security*, 1(3), 154–160.
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. doi:10.1109/TIT.1976.1055638
- Gupta, D. S., & Biswas, G. P. (2015a). Securing Voice Call Transmission over Cellular Communication. *Procedia Computer Science*, 57, 752–756. doi:10.1016/j.procs.2015.07.469

- Gupta, D. S., & Biswas, G. P. (2015b). Secure Computation on Cloud Storage: A Homomorphic Approach. *Journal of Cases on Information Technology*, 17(3), 22–29. doi:10.4018/JCIT.2015070103
- Gupta, D. S., & Biswas, G. P. (2015c). Identity-Based/Attribute-Based cryptosystem using threshold value without Shamir's Secret Sharing. In *Signal Processing, Computing and Control (ISPCC), 2015 International Conference on* (pp. 307–311). IEEE.
- Gupta, D. S., & Biswas, G. P. (2016). Cryptanalysis of Wang et al.'s lattice-based key exchange protocol. *Perspectives on Science*, 8, 228–230. doi:10.1016/j.pisc.2016.04.034
- Gupta, D. S., & Biswas, G. P. (2017). A secure cloud storage using ECC-based homomorphic encryption. *International Journal of Information Security and Privacy*, 11(3), 54–62. doi:10.4018/IJISP.2017070105
- Gupta, D. S., & Biswas, G. P. (2017a). An ECC-based authenticated group key exchange protocol in IBE framework. *International Journal of Communication Systems*, 30(18), e3363. doi:10.1002/dac.3363
- Gupta, D. S., & Biswas, G. P. (2017b). On securing bi-and tri-partite session key agreement protocol using ibe framework. *Wireless Personal Communications*, 96(3), 4505–4524. doi:10.1007/11277-017-4399-5
- Gupta, D. S., & Biswas, G. P. (2018b). A novel and efficient lattice-based authenticated key exchange protocol in C-K model. *International Journal of Communication Systems*, 31(3), e3473. doi:10.1002/dac.3473
- Gupta, D. S., Biswas, G. P., & Nandan, R. (2018a). Security weakness of a lattice-based key exchange protocol. In *2018 4th International Conference on Recent Advances in Information Technology (RAIT)* (pp. 1–5). IEEE. 10.1109/RAIT.2018.8389018
- Hölbl, M., Welzer, T., & Brumen, B. (2012). An improved two-party identity-based authenticated key agreement protocol using pairings. *Journal of Computer and System Sciences*, 78(1), 142–150. doi:10.1016/j.jcss.2011.01.002
- Jeong, I. R., Katz, J., & Lee, D. H. (2004, June). One-round protocols for two-party authenticated key exchange. In *International Conference on Applied Cryptography and Network Security* (pp. 220–232). Springer. 10.1007/978-3-540-24852-1_16
- Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209. doi:10.1090/S0025-5718-1987-0866109-5
- Liu, Y., Cheng, C., Cao, J., & Jiang, T. (2012). An improved authenticated group key transfer protocol based on secret sharing. *IEEE Transactions on Computers*, 62(11), 2335–2336. doi:10.1109/TC.2012.216
- McCullagh, N., & Barreto, P. S. (2005, February). A new two-party identity-based authenticated key agreement. In *Cryptographers' Track at the RSA Conference* (pp. 262–274). Springer. 10.1007/978-3-540-30574-3_18
- Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO'85 Proceedings* (pp. 417–426). Springer.
- Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques* (pp. 47–53). Springer.

Tseng, Y. M. (2007). An efficient two-party identity-based key exchange protocol. *Informatica*, 18(1), 125–136.

ADDITIONAL READING

Bellare, M., & Rogaway, P. (1993, December). Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security* (pp. 62–73). ACM. 10.1145/168588.168596

Dang, L., Xu, J., Cao, X., Li, H., Chen, J., Zhang, Y., & Fu, X. (2018). Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks. *International Journal of Distributed Sensor Networks*, 14(4), 1550147718772545. doi:10.1177/1550147718772545

ElGamal, T. (1984). A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in cryptology* (pp. 10–18). Springer Berlin Heidelberg.

Gupta, D. S., & Biswas, G. P. (2018). Design of lattice-based ElGamal encryption and signature schemes using SIS problem. *Transactions on Emerging Telecommunications Technologies*, 29(6), e3255. doi:10.1002/ett.3255

Gupta, D. S., & Biswas, G. P. (2018). On Securing Cloud Storage Using a Homomorphic Framework. In *Technology Management in Organizational and Societal Contexts* (pp. 99–114). IGI Global. doi:10.4018/978-1-5225-5279-6.ch005

Kumar, M. (2019). AOR-ID-KAP: An Authenticated One-Round Identity-Based Key Agreement Protocol for Wireless Sensor Network. In *Computational Intelligence in Sensor Networks* (pp. 427–454). Berlin, Heidelberg: Springer. doi:10.1007/978-3-662-57277-1_18

Lei, X., & Liao, X. (2013). NTRU-KE: A Lattice-based Public Key Exchange Protocol. *IACR Cryptology ePrint Archive*, 2013, 718.

Liao, L. (2007). *Group key agreement for ad hoc networks*. VDM Verlag.

Mukherjee, S., Gupta, D. S., & Biswas, G. P. (2018). An efficient and batch verifiable conditional privacy-preserving authentication scheme for VANETs using lattice. *Computing*, 1–26.

Ni, L., Chen, G., Li, J., & Hao, Y. (2011). Strongly secure identity-based authenticated key agreement protocols. *Computers & Electrical Engineering*, 37(2), 205–217. doi:10.1016/j.compeleceng.2011.03.001

Wang, S., Cao, Z., Choo, K. K. R., & Wang, L. (2009). An improved identity-based key agreement protocol and its security proof. *Information Sciences*, 179(3), 307–318. doi:10.1016/j.ins.2008.09.020

KEY TERMS AND DEFINITIONS

Authentication: Permission to access something, which is confidential. The authentication is only provided to authentic users.

Cryptography: The art and science of creating unreadable messages from readable messages by the need of security.

Decipherment: The inverse of encipherment which is also an algorithm to change unreadable messages to readable messages.

Elliptic Curve: A curve in two dimensions, which is known by its group property on points. It is widely used in cryptography due to its hard assumptions.

Encipherment: An algorithm used to convert a readable message into unreadable message. It is used in the field of security.

Key Exchange: A method of transferring a secret key among various users. This key may be needed in cryptography to protect many entities like information, system, etc.

Secure Communication: A method of transferring information on the internet securely.

Efficiency Issues and Improving Implementation of Keystroke Biometric Systems

Ali Kartit

 <https://orcid.org/0000-0002-3472-1151>

LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco

Farida Jaha

LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco

INTRODUCTION

Employees use more and more their mobile devices in work specifically after having introduced a new trend called BYOD (Bring Your Own Devices) that allows workers to provide their own devices and use the same materials for both personal and professional purposes. This new practice improves employee productivity by using of a mastered mobile device and it decreases the budget spent on IT because the materials used are purchased and maintained by employees at the same time it offers disadvantages like security issues. Therefore, it is very important to use an authentication platform like authentication based on knowledge (password, etc.), physical biometric authentication (iris, etc.) or behavioral biometric authentication (keystroke dynamics, etc.) to avoid data leakage.

This paper deals with biometric authentication based on keystroke dynamics. The method consists of analyzing the typing patterns of a claimed user and then decide to accept or reject the user authentication attempt.

The main advantages of keystroke dynamics are: (1) it improves productivity by using a known device, (2) As the user is typing his login and password; biometric data is extracted and compared to a reference profile stored in the system database without the need of an extra time to verify the user, (3) it allows a reduction in investment, it does not require external hardware. The keystroke dynamics implementation is based essentially on software, which is the subject of this paper.

keystroke can be integrated into several applications, whether web applications, behavioral intrusion detection system, online banking, etc. Its flexibility comes from the fact that the administrators of its systems do not have to force the user to buy additional equipment (e.g fingerprint capture, iris capture, voice capture, etc.) to read the end user's biometric data.

The paper sections are organized as follows: the first section is the methodology followed in the article where we presented the keystroke dynamics technique with its characteristics and the sensors used in the software (dwell time and digraph time). In the same section, we also mentioned some real-world application of this technique and finally the architecture adopted in the development of the software. The second section is the proposed work in which the four phases (registration, enrollment, authentication and classification) have been detailed. We then treated the setting part and the error metrics that we will use to test the accuracy of the software.

DOI: 10.4018/978-1-5225-9715-5.ch077

BACKGROUND

Keystroke dynamics was and remains a strong field for research, the first documented research published by Forsen, Nelson and Staron (1977) dated back to 1977. Later, many other papers were appeared. For instance, Patil and Renke (2016) published a paper where they better cleared up keystroke dynamics, they mentioned some drawback of this biometric method and they distinguished two different keystroke dynamics authentications: static and continuous. In static, the user is asked to type his login and password, then he is validated by comparing those data with his pre-calculated profile. In the continuous authentication, the end-user's biometric data is captured throughout the use of the system. The use of the second kind of authentication prevents an impostor from taking control of the machine when its legal user is absent (several users leave their workstations without locking them or putting them in sleep mode). In this case keystroke recognition can be used as a behavioral intrusion detection system. Grant Pannell and Helen Ashman (2010) combined a set of factors including CPU usage, sites visited and keystroke biometric to implement a behavioral IDS to detect unauthorized users through their system usage. On the same page, Avasthi and Sanwal (2016) gave the existing approaches, security and challenges of keystroke dynamics in order to motivate the researches to further come with more innovative improvements. Some other researchers like Panasiuk, Dabrowski, Saeed, and Bochenska-Wlostowska (2014) devoted their studies to compare different keystroke dynamics databases and to test if the same algorithm running on two theoretically identical databases gives the same results.

Other research tried to improve the EER (Error Equal Rate) and the security level of the devices using keystroke biometric like Morales, Falanga, Fierrez, Sansone, and OrtegaGarcia (2015) team and Nagargoje, Lomte, Auti, and Rokade (2014) team who combined keystroke and mouse movement to authenticate the user and increase the device confidentiality.

Systems with touchscreens, which are replacing more and more traditional computer systems, arouse researchers like Kambourakis, Damopoulos, Papamartzivanos, and Pavlidakis (2014). They try to adapt keystroke dynamics authentication to this kind of screen. Teh, Zhang, Teoh, and Chen (2016) gave us an overview and survey of a touch dynamics authentication system available for devices with touchscreen.

Morales, Fierrez and Tolosana (2016) focused on reporting the results of 31 different algorithms evaluated according to accuracy and robustness.

Liakat, Monaco, Tappert and Qiu (2017) presented a detailed survey of the most recent researches on keystroke dynamic authentication. They analyzed different methods, algorithms used, the accuracy rate, and the shortcomings of those investigations. In the same direction, Teh, Zhang, Teoh and Chen (2016) presented a survey of user authentication using keystroke dynamics.

Further, new studies are focused on analyzing keystroke recognition method for smartphones such as Ho's research published in 2014 and later Alzubaidi and Kalita in 2015, they highlight some problems that concern smartphones security in fact that smartphones are small in size and they can easily be lost or be stolen which increases the need to use two-factor authentication. Different research has shown that keystroke dynamics can be adapted to different systems. For example, Antal, Szabo, and László (2015) demonstrated experimentally, using Android devices, that touchscreen-based features improve keystroke dynamics based identification and verification. Boakye and Marfo (2016) determined the effectiveness of keystroke analysis and password security synergy to authenticate users of a system web-based applications. Another example to give is Babaeizadeh, Bakhtiari, and Maarof (2014) who address using keystroke authentication in mobile cloud computing.

Our Contribution

1. Most available software in keystroke dynamics fields use Euclidean distance in their algorithm. However, according to the team research composed of Panasiuk, Dabrowski, Saeed, and Bochenska-Wlostowska(2014) and the team composed of Antal, Szabo, and László (2015), k-Nearest Neighbor (K-NN) and Manhattan distance are the most top-performing methods comparing with the Euclidean distance. Which makes the software using the last method less precise and the results obtained less exact.

Thus, to improve the keystroke algorithm, we use k-Nearest Neighbor (K-NN) as a classification method. KNN, a straightforward classifier, has been used in statistical estimation and pattern recognition. It identifies the k closest neighbors of feature value. In our case, we use 1-NN to search one nearest neighbor of a user's typing pattern.

In addition, we adopt K-NN and K-FN (K-Further Neighbor) algorithm based on Manhattan distance instead Euclidean distance to calculate the distance between the claimed user typing pattern and the original user feature values.

2. Most research remains theoretical. In this paper, we propose a complete software that can be used in mobile devices that need a biometric system for authentication besides password especially devices without two-factor authentication method. The software is based on the pseudo code already discussed in our previous paper Jaha and Kartit (2017).

METHODOLOGY

Keystroke Dynamics

The authentication process validates the identity of the user who is trying to connect to the system. Most traditional systems are based on a login and password to grant or not access to the device whether it is a computer, smartphone, e-mail, cloud or e-commerce. This kind of authentication belongs to the category of knowledge-based authentication. For companies and information technology systems, whose data is sensitive, critical and does not support identity theft or data leakage, the use of single-factor authentication such as password-based authentication can cause them many security problems. Thus, they use more sophisticated authentication methods such as ownership-based authentication (e.g access card), and biometric-based authentication (e.g keystroke dynamics).

The biometric-based authentication divided into two parts: physiological such as fingerprint identification and retina scan, and behavioral like voice recognition and keystroke dynamics recognition. To choose the appropriate authentication method, the IT system administrator can refer to the following criteria:

- The IT budget.
- The level of security that the administrator wants to apply in the company (high, medium, low).

Keystroke recognition is a biometric technique which can automatically identify a person by typing his login and password. It describes exactly when each key was pressed and when it was released the time a device user is typing.

We chose keystroke biometric because of its many characteristics, including:

- **Uniqueness:** Each of us has his own way of typing that differs from another person so even if another user has discovered the password via hacking techniques such as brute force attack or shoulder surfing attack. the password will be useless to him because the two users have two different typing profiles.
- **Reduced Cost:** We do not need to buy an external device we just need the keyboard and software that captures the user's biometric information unlike other methods that require an external device.
- **Simplicity of implementation:** to implement Keystroke dynamics we need to capture and save the user's biometric data and save his typing profile. many algorithms are used to implement keystroke such as the example of a CREYC algorithm based on Euclidean distance and the algorithm discussed in this paper based on K-NN and Manhattan distance. The most important thing is that the code is feasible and can be integrated into different applications requiring authentication such as windows applications, web applications, social networks, online banking, e-commerce, etc.
- **Easy Updating:** Keystroke dynamic changes with age or after some diseases in this case just ask the user to retype his login and password to capture his new biometric data.

There are many keyboard features can be used to authenticate a person using typing pattern: keystroke pressure, keystroke speed, typing sound, dwell time and flight time.

Studies conducted by Kaur and Virk in 2013 and those of Morales, Fierrez, Tolosana, Ortega-Garcia, Galbally, Gomez-Barrero, ... and Marcel in 2016 demonstrate that the use of dwell time and digraph times (flight times) gives the best FAR (False Acceptance Rate) and FRR (False Rejection Rate) combination. Therefore, for identifying the genuine user from impostors, we have adopted dwell time noted f_i^d and different digraph times noted f_i^{L1} , f_i^{L2} and f_i^{L3} in which:

- f_i^d : Is the time interval between consecutive key press and key release
- f_i^{L1} : Is the time difference between releasing the i th key and pressing the $(i+1)$ th key.
- f_i^{L2} : Is the time difference between the pressure of the i th button and pressure the $(i+1)$ th button.
- f_i^{L3} : Is the time difference between the release of the i th key and the release of $(i+1)$ th key.

Real-World Applications of Keystroke Dynamics

The first application field of keystroke dynamics is security. Keystroke dynamics allows us to adopt two-factor authentication by combining the knowledge-based authentication and biometric-based authentication. One of the advantages of this technique is that the system administrator will not have to create and apply a password policy to force the user to change his password after a certain period of use and the employees can keep the same passwords. they can also use weak passwords without respecting the password complexity requirements without creating a vulnerability in the IT system (the hacker, even if he knows the password, must simulate the typing profile of his victim).

Besides using keystroke dynamics to authenticate a system user in order to increase the level of security and filter out unauthorized users, the application areas for dynamic typing remain numerous and varied.

The keystroke recognition approach can be used in the field of medicine as illustrated in very interesting paper published by Adams W. R. (2017). In this paper, he discussed the possibility of using keystroke

dynamics for the early detection of Parkinson's disease. The study collected biometric data from people who are affected by Parkinson's disease and from other healthy people. The dataset is analyzed and then transformed into graphs to determine a predicted probability. The same concept is applied by other research conducted by Arroyo-Gallego, T., Ledesma-Carbayo, M. J., Sánchez-Ferro, A., Butterworth, I., Mendoza, C. S., Matarazzo, M., ..., and Giancardo, L. (2017). the latest research focused on early detection of the disease using this time the touch screen instead of keyboard. The most important thing that can be deduced from these studies is that the patient can know if there is a probability of being affected without medical assistance and without the need for external equipment.

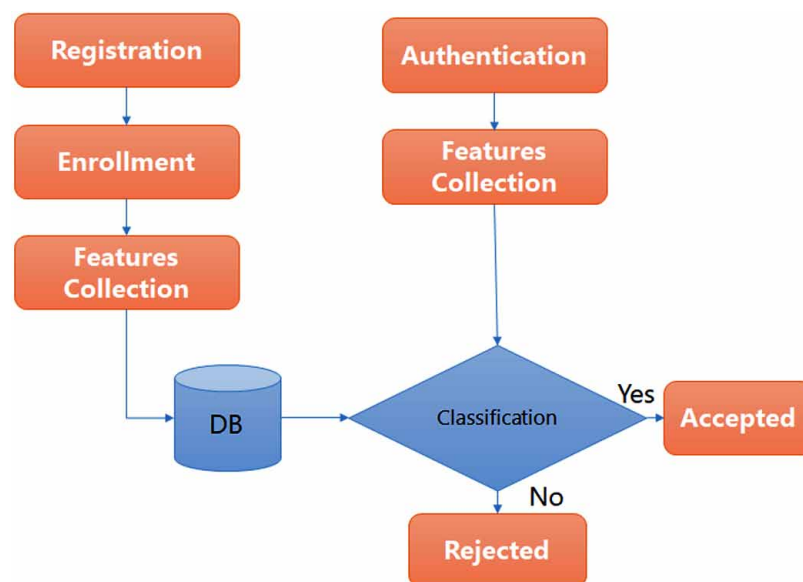
Keystroke dynamics recognition as a behavioral-based authentication, several researchers have integrated the method into behavioral intrusion detection system. Grant Pannell and Helen Ashman (2010) proposed an IDS that combines several factors (mentioned above) including keystroke biometric. the IDS makes it possible to detect abnormal manipulations of the system. the research proposes an H-IDS (host-based intrusion detection) that is installed on each machine to detect usage violations. Similarly, Bondada, M. B. and Bhanu S. M. S. (2014) proposed using an IDS based on keystroke dynamics to detect identity theft and criminal activity that a cloud can be exposed to.

Proposed Work Architecture

Figure 1 shows the general approach used in this study. During his first access to the computer system, the user has to create his own account (Registration phase) and then he is asked to type his login and his password n times (enrollment phase). As the user types, the system records his biometric features (features collection) and stores his reference profile in the system database.

At every attempt of connection to the system, the software captures and recalculates the keystroke biometric of claimed user (authentication phase). This phase involves the use of a classification method; we have used KNN with Manhattan distance, to compare new data against the recorded signature (classification phase). Then, the user will be accepted or rejected based on a predetermined threshold value.

Figure 1. Keystroke dynamics architecture



PROPOSED WORK

We transformed the theoretical framework discussed above to a software divided on different windows, each of them presents one of the phases quoted in the methodology section. The code is written in C# using Microsoft Studio 2015 and we evaluated and analyzed the software using laptop keyboard.

Registration

The registration process is the first step to accomplish before reaching other phases. The user must fill some information including, his full name, his login and password that will be used to authenticate to the system, his gender, his date of birth, and his full address. The account created will be used in authentication and enrollment phases. Those Data will be stored in the system database for future use.

Enrollment Phase and Features Collection

The next step is enrollment phase; the user clicks on the enrollment button to begin the features collection process. Most research capture features data for user password only, in our software we propose to record biometric data during all identification and authentication processes in order to increase the extracted features which means more accuracy. Figure 2 is a screenshot demonstration of user biometric data; the password tested is “ensajschool”.

The user must type his login and password several times. Enrollment attempts is determined by the administrator. In our example, we have chosen 20 as the number of enrollment attempts. The system administrator can increase or decrease the value in setting window.

While the user is typing on keyboard for submitting samples, the software records when keys were pressed and were released to calculate user features like dwell time, digraph time 1, digraph time 2 and digraph time 3. The stored profile will be noted "fg" for genuine user and it represents the reference profile that we will use in classification phase.

Typing login and password containing letters and digits required pressing letters, digits and special keys (tab key to move cursor to the password textbox, caps lock key or shift key to type digits and del or backspace in case of error). By default, the software collects the time functions of all keys, including special keys such as: tab, shift, del, backspace, caps lock... Which gives a false length of typed data. The length value is an essential parameter for a good functioning of the algorithm. That's why we configured the software to ignore these keys.

Figure 2 shows different graphs for dwell time and digraph times, we record those function for the 17 logins and password keys.

Authentication

Each access to the system requires an identification and authentication. Identification allows answering the question: “Who are you?”. It is a phase of establishing the identity of the user. The user uses an identifier called “username” or “login” that identifies and assigned to him individually. Authentication intervenes after the so-called identification phase. It is a phase that allows the user to provide proof of identity. It answers the question: “Are you really this person?” The user uses an authentication method (authentication based on knowledge, physical biometric authentication or behavioral biometric authentication).

Figure 2. Dwell time and flight times of user



During this phase, we record and calculate the user biometric data f_i^d (Press key1-Release key1), f_i^{L1} (Release key1-Press key2), f_i^{L2} (Press key1 – Press key 2) and f_i^{L3} (Release key 1 – Release key 2). Those functions present the user's temporary profile that will be noted "fc" for claimed user.

Classification

Classification phase is the most important step, it answers the following question is the claimed user the original user or an impostor?

According to Banerjee and Woodard (2012), There are many classification methods can be used in keystroke dynamic field specially in classification phase. They categorized those methods into four categories: (1) statistical algorithms based on distance measurement like Euclidean distance and Manhattan distance. (2) Artificial neural network inspired by biological neurons working, adapted later to the field of statistics and then used on Behavioral Biometrics. the examples of this method are backpropagation, sum-of-products and hybrid sum-of-products. (3) Pattern Recognition which is the process of recognizing patterns by using machine learning algorithm such as the nearest neighbor algorithms and SVM (Support Vector Machine). (4) Search Heuristics algorithms such as Particle Swarm Optimization, Ant Colony optimization and Genetic Algorithms.

We chose pattern recognition by using K-NN and K-FN based on Manhattan distance. We have already explained the reason for choosing these two methods and why we opted for Manhattan distance instead of Euclidean distance (Jaha and Kartit (2017)).

To decide if the user will be allowed or rejected we have to:

1. Calculate de Manhattan distance, based on the equation (a), between f_i^d , f_i^{L1} , f_i^{L2} and f_i^{L3} of the temporary profile and each f_{ij}^d , f_{ij}^{L1} , f_{ij}^{L2} and f_{ji}^{L3} captured during enrollment phase according to the equation (b).

$$\sum_{i=1}^n |x_i - y_i| \quad (a)$$

$$D_i = \begin{cases} \sum_{j=1}^k |fg_{ij}^d - fc_i^d| \\ \sum_{j=1}^{k-1} |fg_{ij}^{\partial} - fc_i^{\partial}| \end{cases} \quad (b)$$

with: $\partial \in \{11, 12, 13\}$

$k=1, \dots, K$: number of pressed keys.

$i=1, \dots, n$: number of enrollment attempts.

2. We have to choose the 1-NN (One-Nearest Neighbor), the K factor in our case is equal to 1, by selecting the one minimum Manhattan distance $D_{\min}(c)$ from all D_i , with $i=1, \dots, n$, of all feature acquisitions stored in enrollment phase.

$$D_{\min} = \text{MIN}(D_i(f^{\partial})), \text{ with } \partial \in \{d, 11, 12, 13\} \quad (c)$$

3. We have also to calculate 1-FN (One-Furthest Neighbor) by determining the one maximum Manhattan distance $D_{\max}(d)$ from all D_i .

$$D_{\max} = \text{MAX}(D_i(f^{\partial})), \text{ with } \partial \in \{d, 11, 12, 13\} \quad (d)$$

4. Then we compare $D_{\max}$ and $D_{\min}$ with thresholds, so if the $D_{\max} \leq \text{MAX}_{\text{Threshold}}$ and $D_{\min} \leq \text{MIN}_{\text{Threshold}}$ the user will be accepted else the user will be rejected.

The reason to add F-NN to the classification phase is to better identify the genuine user and determine the lower and upper limits not to exceed.

Setting

We allowed the administrator to change some parameters to improve the result accuracy. These changes are made either to increase the security of access, or to allow a tired or sick user whose typing pattern is changing to access his system.

In the setting windows administrator can modify the following parameters:

1. The password length has an important effect to decrease the software's FAR and FRR. The longer the password is, the better we can capture the user features. Thus, longer phrase allowed obtaining much better accuracy.
2. According to Liakat, Monaco, Tappert and Qiu research threshold has to be variable. One of the conclusions this team reached is that using individual thresholds could improve the performance of the system. For our implementation, we calculated a threshold for each user using the same algorithm used in the authentication phase.

3. The next parameter is the number of entries used to generate the reference patterns, so a user's template is created. What we said for the password applies to number of enrollment attempts which has to be more than 10 times to capture a different states of mind of the user (comfortable, tired, etc.).
4. The last parameter is number of authentication, the user has not an infinite authentication attempts. The administrator can increase or decrease the authentication attempts to give more security for the system against impostor and another attempt for the genuine user to type his login and password correctly with the same rhythm as stored in the system database.

To validate and evaluate this biometric system, we used some error metrics adopted in most biometric systems to evaluate their accuracy. Therefore, we added a statistical section containing four graphs will present the following performance measures (see figure 3):

- FRR is the likelihood that the system will reject an authorized access attempts by the genuine user. FAR is the Percentage of attackers who are accidentally accepted. These two parameters are interlinked if the FAR goes down the FRR will go down and vice versa, the intersection value of these two graphs presents EER. Therefore, we have gathered these three parameters into a single graph in order to be able to determine the EER. The equations adopted to calculate each of these parameters are as follows:

$$FRR = \frac{FN}{FN + TP} \quad (e)$$

$$FAR = \frac{FP}{FP + TN} \quad (f)$$

Here, FP: False positive (imposter scores exceeding threshold), FN: False Negative (imposter scores exceeding threshold), TN: True Negative (imposter correctly rejected) and TP: True Positive (genuine correctly accepted)

- Sensitivity (Se) which is the proportion of true positives among total participants in the test. It is the ability of the software to correctly identify genuine. in statistics, Sensitivity is the true positive rate and in terms of equation, it's:

$$Se = \frac{TP}{TP + FN} \quad (g)$$

- Specificity (Sp) is the rate of impostors correctly detected (true negative). We calculated this value using the equation (h)

$$Sp = \frac{TN}{TN + FP} \quad (h)$$

- Accuracy (Acc) is the power and the ability of the software to distinguish the genuine users from imposters. We used (i) to determinate the software Accuracy value:

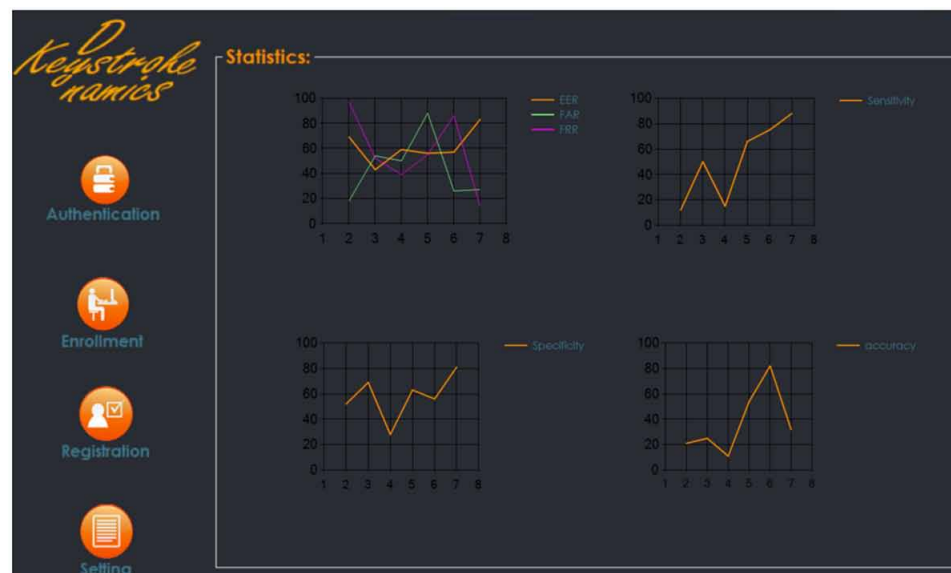
$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \quad (i)$$

We intend to capture the biometric data of 100 participants (98 students and two teachers). The age of the participants varies between 18 and 33 with an average of 19.27. for the moment we are in the data collection phase to obtain at the end of the process a dataset that we will use to evaluate the current software based on K-NN.

FUTURE RESEARCH DIRECTIONS

Our next steps will be: (1) We will improve the software by optimizing the code for faster response time, and by adding some other useful features for the user and system administrator. (2) Since the quality of each biometric system is characterized by FAR, FRR EER, sensitivity, specificity and accuracy, we added a new statistic window dedicated to calculating those error metrics to examine performance and the quality of the software. For the time being, we have completed the programming phase and we are in the phase of data collection from the participants and creating the dataset. The result will be published in our next publication. (3) In order to conclude which method between K-NN using Manhattan distance and Euclidean distance gives the lower FAR, FRR and EER results, we will use the current code and replace K-NN with Euclidean distance then we will compare FAR, FRR and EER of the two methods.

Figure 3. Statistics window



CONCLUSION

5

This paper presented an Improving implementation of keystroke dynamics using KNN and Manhattan distance. We have discussed keystroke's biometric architecture and phases (registration, enrollment, authentication and classification) and showed the logic followed to transform the pseudo code, which we presented in a previous article (Jaha and Kartit (2017)), to operational software. We discussed also the mathematical equations used in the development of the software and we have specified the next step of our research that you can find in the future research directions section.

REFERENCES

- Adams, W. R. (2017). High-accuracy detection of early Parkinson's Disease using multiple characteristics of finger movement while typing. *PLoS One*, 12(11), e0188226. doi:10.1371/journal.pone.0188226 PMID:29190695
- Alzubaidi, A., & Kalita, J. (2015). Authentication of Smartphone Users Using Behavioral Biometrics. *Journal of IEEE Communications Surveys and Tutorials*.
- Antal, M., Szabo, L. Z., & László, I. (2015). Keystroke dynamics on Android platform. *Procedia Technology*, 19, 820–826. doi:10.1016/j.protcy.2015.02.118
- Arroyo-Gallego, T., Ledesma-Carbayo, M. J., Sánchez-Ferro, A., Butterworth, I., Mendoza, C. S., Matarazzo, M., & Giancardo, L. (2017). Detection of Motor Impairment in Parkinson's Disease via Mobile Touchscreen Typing. *IEEE Transactions on Biomedical Engineering*, 64(9), 1994–2002. doi:10.1109/TBME.2017.2664802 PMID:28237917
- Avasthi, S., & Sanwal, T. (2016). Biometric Authentication Techniques: A Study on Keystroke Dynamics. *International Journal of Scientific Engineering and Applied Science*, 2(1), 215–221.
- Babaeizadeh, M., Bakhtiari, M., & Maarof, M. A. (2014). Keystroke Dynamic Authentication in Mobile Cloud Computing. *International Journal of Computer Applications*, 90, 29–36.
- Banerjee, S. P., & Woodard, D. L. (2012). Biometric Authentication and Identification using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research*, 7(1), 116–139. doi:10.13176/11.427
- Boakye, O. M., & Marfo, Y. M. (2016). Utilizing Keystroke Dynamics as an Additional Security Measure to Password Security in Computer Web-based Applications - A Case Study of UEW. *International Journal of Computers and Applications*, 149(5), 35–44. doi:10.5120/ijca2016911402
- Bondada, M. B., & Bhanu, S. M. S. (2014). Analyzing User Behavior Using Keystroke Dynamics to Protect Cloud from Malicious Insiders. *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 1–8. 10.1109/CCEM.2014.7015481
- Forsen, G., Nelson, M., & Staron, R., Jr. (1977). *Personal attributes authentication techniques*. Technical Report RADC-TR-77-333. Rome Air Development Center.
- Gascon, H., Uellenbeck, S., Wolf, C., & Rieck, K. (2014). *Continuous authentication on mobile devices by analysis of typing motion behavior*. GI Conference Sicherheit (Sicherheit, Schutz und Verlässlichkeit).

Ho, G. (2014). *Tapdynamics: strengthening user authentication on mobile phones with keystroke dynamics*. Technical report. Stanford University.

Jaha, F., & Kartit, A. (2017). Pseudo code of two-factor authentication for BYOD. *2017 International Conference on Electrical and Information Technologies (ICEIT), IEEE Conferences*, 1 – 7.

Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E. (2014). Introducing touchstroke: Keystroke-based authentication system for smartphones. *Security and Communication Networks*.

Kaur, M., & Virk, R. S. (2013). Security System Based on User Authentication Using Keystroke Dynamics||. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(5), 2111–2117.

Liakat, M. A., Monaco, J. V., Tappert, C. C., & Qiu, M. (2017). Keystroke Biometric Systems for User Authentication. *Journal of Signal Processing Systems for Signal, Image, and Video Technology*, 86(2-3), 175–190. doi:10.1007/11265-016-1114-9

Mhenni, A., Rosenberger, C., Cherrier, E., & Essoukri Ben Amara, N. (2016). Keystroke Template Update with Adapted Thresholds. *International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Monastir, Tunisia. DOI: 10.1109/ATSIP.2016.7523122

Morales, A., Falanga, M., Fierrez, J., Sansone, C., & OrtegaGarcia, J. (2015). Keystroke Dynamics Recognition based on Personal Data: A Comparative Experimental Evaluation Implementing Reproducible Research. *Proc. of the IEEE Seventh Int. Conf. on Biometrics: Theory, Applications and Systems*, 1-6. 10.1109/BTAS.2015.7358772

Morales, A., Fierrez, J., Tolosana, R., Ortega-Garcia, J., Galbally, J., Gomez-Barrero, M., ... Marcel, S. (2016). Keystroke Biometrics Ongoing Competition. *IEEE Access: Practical Innovations, Open Solutions*, 4, 7736–7746. doi:10.1109/ACCESS.2016.2626718

Nagargoje, Y. R., Lomte, S. S., Auti, R. A., & Rokade, A. H. (2014). Security using Fusion of Keystroke and Mouse Dynamics, *International Journal Of Scientific. Research in Education*, 2(7), 1185–1194.

Panasiuk, P., Dabrowski, M., Saeed, K., & Bochenska-Wlostowska, K. (2014). The Comparison of the Keystroke Dynamics Databases. In *13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM)*. Ho Chi Minh City, Vietnam: Springer. 10.1007/978-3-662-45237-0_13

Pannell, G., & Ashman, H. (2010). Anomaly Detection over User Profiles for Intrusion Detection. In *8th Australian Information Security Management Conference*. Edith Cowan University.

Patil, R. A., & Renke, A. L. (2016). Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm. *International Journal of Computers and Applications*, 144(9), 27–33. doi:10.5120/ijca2016910432

Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. K. (2016). A survey on touch dynamics authentication in mobile devices. *Computers & Security*, 59, 210–235.

Zhong, Y., & Deng, Y. (2015). *Recent Advances in User Authentication Using Keystroke Dynamics*. Science Gate Publishing. DOI: . doi:10.15579/gcsr.vol2.ch4

ADDITIONAL READING

5

Alsultan, A., & Warwick, K. (2013). Keystroke dynamics authentication: A survey of free-text methods. *International Journal of Computational Science*, 10(4), 1–10.

Liakat, M. A., Monaco, J., Tappert, C., & Qiu, M. (2015). Authentication and identification methods used in keystroke biometric systems. In *IEEE international symposium on big data security on cloud (Big Data Security 2015)* (pp. 1424–1429). IEEE.

Xi, K., Tang, Y., & Hu, J. (2011). Correlation keystroke verification scheme for user access control in cloud computing environment. *The Computer Journal*, 54(10), 1632–1644. doi:10.1093/comjnl/bxr064

Modern Blue Pills and Red Pills

Asaf Algawi

University of Jyväskylä, Finland

Michael Kiperberg

Holon Institute of Technology, Israel

Roe Shimon Leon

University of Jyväskylä, Finland

Amit Resh

Shenkar College, Israel

Nezer Jacob Zaidenberg

College of Management, Israel

INTRODUCTION

Johanna Rutkowska first introduced the concept of the blue pill and the red pill (Rutkowska 2006). The blue pill is a hypervisor-based rootkit that takes control of a victim host computer. A red pill is a software tool designed to detect a blue pill.

A term that is closely related to trusted computing is the attestation concept (Zaidenberg et al. 2015), where a remote host or local software tries to ensure the integrity of the local machine. This concept was also researched by Kennell et al. (2003) in order to establish genuinity of a remote host. (a physical machine running the correct software as opposed to an emulator or a virtual machine or a physical machine running non-genuine software).

Since the introduction of blue pills, many red pills have been designed for their detection; however, more advanced blue pills have been designed to avoid detection.

Today, modern CPUs (such as Intel core iX processors or ARM8 architecture) feature hardware-supported virtualization. Hardware-supported virtualization provides new capabilities to virtual machine and emulators software. Thus, hardware-supported virtualization makes several “red pill” attempts futile. However, hardware-supported virtualization also provides new forensics opportunities and therefore, many new opportunities to create new red pills.

This chapter describes the red pill and blue pill situation on Intel and AMD virtualizations circa 2018 and the eighth generation of core iX CPUs.

BACKGROUND

Blue pill technology relies on hypervisor technology. This chapter reviews recent advances in x86 virtualization. These new instruction families enable blue pill and red pill technologies.

DOI: 10.4018/978-1-5225-9715-5.ch078

Hypervisors and Thin Hypervisors

A hypervisor is a type of computer software designed to run multiple operating systems on the same hardware.

As its name implies, a hypervisor has more permission than the operating system (i.e., the supervisor).

Just like the operating system supervises memory and hardware resources for the processes it runs, the hypervisor controls the hardware resources for each operating system.

Hypervisor research started with Popek et al. (1974) who classify hypervisors into two main categories:

1. Type I hypervisors, or boot hypervisors, are hypervisors that the machine starts from the hardware boot. The machine then starts the guest operating system. VMWare ESXi is an example of a modern Type I hypervisor.
2. Type II hypervisors, or hosted hypervisors, are hypervisors that start only after the operating system has started. A modern example for a Type II hypervisor is VMWare Desktop or Oracle Virtual Box.

Regular hypervisors are situated between the hardware and the supervisor (OS), catching interrupts and controlling memory addresses. The hypervisor decides which operating system owns each memory address and which operating system should handle each hardware interrupt.

There is a particular case of hypervisors that do not attempt to run multiple operating systems. Instead, these hypervisors, called “thin hypervisors”, supports running only one operating system on the target hardware. Thin hypervisors act as a microkernel that provides specific services. The thin hypervisor passes the handling of all (or almost all) hardware events and interrupts to a single operating system. It also includes very little memory management and relies on the guest OS memory management system and interrupt handling. Microsoft’s Deviceguard, TrulyProtect hypervisor for protection against reverse engineering (Averbuch et al. 2013) and Execution Whitelisting (Kiperberg et al. 2017) are examples of thin hypervisors. Virtually all blue pills are thin hypervisors.

x86 Virtualization

The x86 architecture, provide virtualization support by platform-specific instructions. Intel architecture and AMD architecture each provide three families of instructions for handling hypervisors. New processor generations optimize these instructions but their structure remains.

The x86 instructions are presented in Table 1.

Table 1. x86 virtualization instructions

	Intel Name	AMD Name	Usages
Virtual-ization instructions	VT-x	AMD-v	Starting a hypervisor
SLAT (second-level address translation)	EPT (Extended page tables)	RVI (Rapid virtualization indexing)	Multiple MMUs for multiple operating systems
IO MMU	VT-d	IOMMU	Assigning IO memory to specific operating systems
VM data structure	VMCS	VMCB	Holding VM information

Rootkits, Bootkits, and the Blue Pill

Once an attack is detected on any networked server, the recommended System Administrator action is to reinstall the server operating system. If the operating system is reinstalled (and fully patched with security patches), then the hacker may find herself locked outside of the system. It follows that the hacker has a desire to hide their tracks and maintain persistent access to the hacked servers. Therefore, hackers frequently install what is known as a “rootkit.”

A rootkit is a software that allows the hacker access to the victim computer resources. Furthermore, the rootkit hides itself and the processes the hacker runs to mask its existence. The rootkit goals are ease of access to victim computer resources and the best measures to hide its existence.

There are many ways to build rootkits from hijacking system calls and library functions and installing *setuid* programs to replacing innocent-looking binaries.

One of the ways a rootkit may operate is as a bootkit. A bootkit is a type of rootkit that boots (from the hard drive master boot record, UEFI, PXE, or other means) before the operating system starts. The bootkit starts its software before the OS starts and later boots the OS. The bootkit may patch the OS system calls to hide its processes and files.

The blue pill is a particular type of rootkit. Unlike normal rootkits and bootkits that modify the operating system in order to hide files and gain access to the system, the blue pill starts a hypervisor and, thus, gains more permissions than the operating system. The blue pill can run processes in the hypervisor address space that are not visible or swappable by the operating system scheduler.

The Original Blue Pill and Subverting Attacks

Rutkowska (2006) introduced the blue pill concept in 2006. The blue pill approach was an innovative rootkit approach that was relatively unresearched at the time. Since Rutkowska introduced the first blue pill, there have been several suggestions on how a blue pill can be detected (for example, the memory location of the IDT vector) and advances in x86 virtualization technology that make such detection more difficult.

Paranoid Fish And Other Red Pills

Paranoid fish (Pafish) (Ortega 2016) is currently the *de facto* standard red pill for blue pill detection. Pafish includes multiple tests capable of detecting most known blue pills when running under Linux or Windows. Many of the tests to detect a hypervisor assume it is not trying to hide by looking up specific values in memory.

Local timing methods are employed to try to flush out a blue pill. These tests perform the following steps:

1. Take the local time (for example, RDTSC instruction).
2. Execute an operation that must be intercepted by a hypervisor (for example, CPUID instruction).
3. retake the local time again to obtain elapsed time.

The underlying assumption is that step (2) takes significantly longer when a hypervisor is active. The elapsed time is compared against a threshold to determine if a hypervisor is active.

Blue Chicken

Rutkowska et al. (2007) introduced the blue chicken blue pill one year after the original blue pill. The blue chicken blue pill detects the red pill inspection attempts and unloads itself, and then restarts after the detection attempts are over. The blue chicken method is not recommended today because a hypervisor can be loaded after the blue pill unload itself. Then, if the blue pill tries to reload itself, the new hypervisor can detect it and prevent the blue pill from loading. The new hypervisor can even act as a blue pill, allowing the original blue pill to load and inspect its operational logic.

The Human Factor

Installing a hypervisor on any system has a performance penalty of several per cents. This performance loss occurs even if the hypervisor is not performing any activity. Using a hypervisor introduce a “second level address translation” i.e. when accessing any memory address another memory lookup occurs which has minor performance cost. This is the reason for the minor performance loss.

It is particularly true if a malicious blue pill is running and mining cryptocurrencies or spying on the user or performing other activities.

Humans are using most systems. Since humans have poor ability to measure and compare response times minor performance loss is usually not noticed. Even if the user is familiar with the system (such as a computer one uses daily), it is quite unlikely that they will notice that the system is running 10% slower. Furthermore, in some cases, the target system can be a server that is not commonly used. In these cases, even a performance drop of 30–50% may be undetected as slow responses are attributed to network latencies etc.

In extreme cases of a performance drop, the user may notice something is wrong even without other indications.

In other cases, a system with constant performance evaluation may be running (for example, calculating nodes per second on a graph problem); in such cases, a sudden drop in the system performance will be noticed.

For the red pill to be an efficient detector without too many false positive results, the performance drop must be significant. Minor drops in performance are usually undetectable. In small-scale tests, minor drops can be attributed to interrupts. In larger scale tests, these drops can be attributed to OS patches, other software, etc.

Modern computers are complex systems and regularly receive interrupts and events from multiple sources, software updates etc.; therefore, using small performance drops will result in multiple false positive detections.

REMOTE RED PILLS

“Remote red pills” refers to situations where a trusted third party is available to test the inspected system. These tests make more sense as they do not rely on a system that is considered untrustworthy.

If such a remote system is available, then these tests can attest the system with greater confidence than local tests. Unfortunately, for many real-world cases and scenarios, such reliable third-party systems do not exist.

Kennell's Timing Method and Derived Attacks

Kennell et al. (2003) proposed a method to perform a remote hypervisor red pill based on computation side effects. Such side effects include TLB and cache hits and misses as well as real-world time that the computation consumes.

According to Kennell's method, the attested computer receives a "challenge" (computation request) from a remote server.

The computation of the challenge causes several computational side effects such as TLB hits, TLB misses, cache hits, cache eviction, etc. The challenge contains several stages in which the side effects of the prior stage are added to the computation result and thereby affect the result of the next phase. In order to pass the Kennel test, the tested computer must not only produce the same results for the computation itself but also compute accurate results for the side effects as well. Furthermore, the computation must be completed in a short time (the time it would take a non-virtual machine to calculate). The Kennell test relies on the fact that if a blue pill or an emulator is running the side effects are bound to be different. Thus, the calculation of side effects must be done separately and consume more time. Thus the response to the challenge on an emulated machine or virtual machine is bound to be wrong or arrive too late. The Kennell test will declare that the machine is not genuine in both cases.

Kennell's method came under direct attack the following year. Shankar et al. (2004) claimed that performance side effects are not sufficient as a method for software detection.

Kennell (2004) has answered these claims, and the matter rested until virtualization became commonly available in modern PCs.

Kiperberg et al. (2013) claimed that the Kennell method could be replicated on modern PCs with hardware virtualization. This result was short-lived as Intel changed their caching algorithm the following year. Furthermore, Intel has not shared its caching algorithms.

However, Kennell tests rely on the availability of certain algorithms, such as CPU caching algorithms, which are not commonly available. These algorithms are considered trade secrets. Furthermore, Intel has changed the caching algorithms of their core iX platform between the second and third generations and changed them again to combat the "meltdown" (Lipp et al. 2018) and "spectre" (Kocher et al. 2018) weaknesses. Thus supporting the Kennell tests on modern hardware require reversing the architecture caching algorithm and is difficult and time-consuming. Supporting the Kennell tests on all recent Intel/AMD architectures can be a menial task that calls for further research.

Network-Based Attacks

Because Kennell has shown that several operations take a significantly longer time when a blue pill is running, it is possible to construct a network-based rootkit using other network servers instead of a Kennell-based attestation server.

For example, if a network-based NTP (network time) server is available and can be considered trustworthy, then it is possible to construct a "network-based blue pill."

The network-based red pill scheme is as follows:

1. Query a network time server.
2. Perform instructions that may take significantly longer if a blue pill is present (for example CPUID) * N times.
3. Query the network time server and obtain the difference.

4. Compare the time required to perform CPUID against a threshold.

The time measurements can be done more accurately by pinging other computers in the network as well as the default gateway.

TPM-BASED RED PILLS

The Trusted Platform Module (TPM) is a device that is found on most modern computers. TPM includes several performance counters that take measurements during the system boot.

The TPMs are developed using hardware obfuscation methods that prevent them from being reversed easily.

One of the main goals of the TPM is to attest the hardware and software that are currently running. This is performed using the following steps:

1. Establish a trust nexus.
2. Maintain a chain of trust.
3. Perform TPM attestation (remote and local).

Establishing a Trust Nexus

The TPM chip itself is the trust nexus. The TPM is built using hardware obfuscations, and its internals cannot be easily reversed. Tarnovsky (2010, 2012) has proved that specific TPM models can be attacked; however, there are no known attacks on modern TPM modules. If the risk that a modern TPM chip will be hacked is accepted (or considered negligible), then the TPM can serve as a root of trust (or trust nexus).

Chain of Trust

The TPM is capable of attesting the UEFI BIOS.

Using secureboot, the UEFI BIOS can ensure that the operating system or boot hypervisor boot loader is trusted.

The boot loader can attest the operating system.

The operating system can attest the software that runs on top it.

Thus, barring an unknown operating system bug or 0-day, the chain of trust can attest the software that runs on the end-point, providing that the trust nexus can be attested.

TPM Attestation

TPM supports local and remote attestation.

When a system with TPM boots, performance counters values are calculated and stored in the TPM performance counters. Both methods rely on the correct values to be stored on the TPM performance counter for the

When running a remote attestation, the remote computer sends the attested machine a challenge. The challenge must be encrypted using the correct encryption key, which can only be calculated if the correct values reside in the performance counter. If the correct values reside in the performance counters,

then the root of trust is set. The root of trust should attest the next chain in the chain of trust, and each link in the chain should attest the next link. If the correct values are not found, then it is impossible (at least without brute force attack or breaking the cypher) to provide the correct response to the challenge, and the attestation will fail.

In local attestation, the system is encrypted using a key that can only be obtained on a trusted system.

If the system is not trusted, then it is impossible to decrypt the system and pass the local attestation test.

LOCAL RED PILLS

Local red pills are tests performed by the tested machine and contained within the tested machine. These tests cannot be considered reliable as computation is performed on an untrustworthy machine (the very same machine is both inspecting and being inspected). However, in many real-life scenarios, there is no TPM chip available or similar third party chip or server that one can use for attestation.

If no third party root of trust is available, then one is left with running local code on an untrustworthy machine to provide attestation in a best effort attempt to detect blue pills on the inspected machine.

Paranoid Fish Tests

Paranoid Fish (Pafish) tests include the following:

1. Specific and paravirtualization tests – These tests are designed to detect specific commercial hypervisors (that do not try to hide)
2. Timing tests (Pafish includes two timing tests)
 - a. RDTSC, CPUID, RDTSC < 1000 cycles.
 - b. This test runs in userspace.
 - c. It runs the CPUID instruction, which must be intercepted by a hypervisor. As a result of the required context switch, the time required for the three instructions acts as a tell-tale sign for hypervisor presence (the red pill).
 - d. RDTSC, RDTSC < 750 cycles - This test involves calling two RDTSC instructions and measuring the response times. It is designed to ensure that the hypervisor is not intercepting the RDTSC instruction.
 - e. In both tests, an irregular high result will be obtained due to an intercept or context switch. To avoid false positives due to the irregular time required for the context switch, Pafish performs an average over ten runs.
3. Sandbox tests – These tests detect if the system is some sandbox. The tests measure if there is no user interaction or mouse movement.

Defeating Paranoid Fish Timing Tests

Most Pafish tests can be overcome using the following methods:

1. Instruction replacement – The CPUID operating can be detected and replaced by the hypervisor. In that method, the first time that CPUID is called a context switch will occur and, indeed, take a long time; however, further instructions can be replaced with another instruction that generates a similar response (such as generating an interrupt and returning with IRET).

2. Tampering with RDTSC - The hypervisor is allowed to intercept calls to RDTSC and similar calls and provide its own responses. The hypervisor may run its own code and return values that are smaller than the values obtained from the CPU. These values can take into consideration the time spent in the hypervisor. However, RDTSC time measurements are needed for the operating system to function correctly. Tampering with RDTSC return values may cause system instability.
3. Intel allows the time measurements (in CPU cycles) on the VM to be slower than on the actual machine; for example, every two CPU cycles on the physical PC can be considered as only one CPU cycle on the guest. This method can offset several of the red pill tests as operations no longer take “too much time.”
4. However, this test work with a constant multiplication factor. In real life, a constant multiplication factor does not occur. Some CPU opcodes require context switches and are much slower when a hypervisor is present while other operations take precisely the same amount of time regardless of hypervisor presence. Thus, These tests can be offset by performing operations that do not take longer on a VM (such as ADDing, ORing, and NOPing). It is possible to create a sequence of speedy operations that do not run slower on a VM (operations that do not require address translation, for example logical operations on registers, NOP etc.) . If the VM is running some clock adjustment were VM cycles are slower than real world cycles then these operations are likely to take too little time on the VM. (creating yet another type of red pill)

Augmenting Paranoid Fish

The Pafish timing test runs in user mode and examines only a limited set of instructions (for example, only RDTSC and not RDTSCP). By augmenting Pafish timing tests to run in kernel mode and trying multiple instructions (RDTSC, RDTSCP etc.), the Pafish tests can become more potent and harder to avoid.

Other well-known tests not found in Pafish include verifying the IDT pointer.

Nested Virtualization Tests

One of the tests not performed by Pafish is performing virtualization instructions (calling VMXON, VMREAD etc.) and performing complex virtualization operations such as EPT or IOMMU operations.

These instructions require a specific effort to support nested virtualization. Running these instructions efficiently poses extra complexity on the hypervisor, which is not implemented by some commercial hypervisors such as Oracle’s Virtual Box.

Calling these instructions introduces additional complexity, which the normal blue pill hypervisor may not meet or may not meet within time and complexity limits.

Like the CPUID instructions, all of Intel’s VMX instructions induce an exit from guest to host mode, making it mandatory to emulate and, thus, extending timing attacks to new instruction types and even mixing instructions from the family. Additionally, VMX instructions also modify the flags register in order to notify VMM software of success or failure of the instructions.

TYPES of VMX Instructions

The Intel architecture VMX instructions are presented (AMD instructions are similar). The understanding of these instructions is required in order to understand and overcome VMX instruction-based red pills.

VMXON instruction is used to switch the CPU into VMX mode. This instruction only affects CPU flags if it succeeds or fails.

VMXOFF instruction is used to turn off VMX mode in the CPU. This instruction only affects CPU flags if it succeeds or fails.

VMCLEAR instruction is used to initialize the VMCS control structure. It writes some data into the first 32 bits of the VMCS page while also affecting the CPU flags if it succeeds or fails. Moreover, it clears the running flag from the VMCS.

VMPTRLD instruction is used to load and mark a VMCS control structure as active or inactive. It affects some opaque data in the VMCS and also affects the CPU flags if it succeeds or fails.

VMWRITE instruction is used as an indirect way to write data into the VMCS data structure. It also affects CPU flags if it succeeds or fails.

VMREAD instruction is used as an indirect way to read data into the VMCS data structure. It also affects CPU flags if it succeeds or fails.

VMLAUNCH instruction is used to launch a VM. Other than the fact that it causes a guest VM to begin execution, it also affects CPU flags after the guest VM has finished its execution due to an exit from guest to host mode. This instruction will not allow a VMCS with a running flag to execute.

VMRESUME instruction works similarly to VMLAUNCH except it will only allow a VMCS, which is marked as running to execute. Additionally, this instruction also affects the CPU flags if it succeeds or fails.

INVEPT instruction causes the CPU to drop cached translations associated with some (or all) EPT pointers stored in the TLB. The instruction also affects the CPU flags if it succeeds or fails.

INVVPID instruction causes the CPU to drop cached translations associated with the VPID pointers stored in the TLB. The instruction also affects the CPU flags if it succeeds or fails.

Defeating VMX Instruction Timing Tests

Timing attacks may be defeated in two ways: either by replacing instructions or by using the capabilities of the VMM in order to lie to the guest about how much time has passed before and after instruction execution.

Defeating VMX Instruction Behavioural Tests

VMX instruction behavioural attacks test the correctness of instruction execution. By following the CPU manufacturer's developer manual, an attacker can see what the correct behaviour of instruction is and which cases cause the instruction to fail or succeed and test each of these cases. The blue pill software role would be to make sure that each of these cases behaves according to the developer manual. If the attacker observes a case that behaves differently, then it can safely assume some VMM software controls the machine. Another class of behavioural test red pill might try actually to execute a virtual machine on its own.

Any VMX instruction operates the same when it comes to success or failure, clearing the CF, ZF, and OF flags in the flags register in case of success or setting them in case of some error.

In some cases, it is required by the blue pill software to save some state between each VMX instruction. These instructions include all those instructions that modify the VMCS directly or indirectly. In the following paragraphs, it is explained how a blue pill software can handle each of these VMX instructions.

VMPTRLD instruction should store the physical address given as its parameter for future use. Storing this value allows the blue pill software to make sure VMREAD and VMWRITE instructions, which require a previously loaded VMCS, also allow the VMCLEAR instruction to behave correctly as VMCLEAR's parameter is an active VMCS. The VMCS stored during the emulation of this instruction will be denoted as L_{12} VMCS, meaning it was created by some hypervisor running at emulation level one and describe a VM that will run at level two while level zero denotes the blue pill hypervisor.

VMCLEAR instruction will clear the running flag of a given VMCS. Because the VMCS structure is opaque and unknown to the red pill software, one can save this flag onto the VMCS itself to mandate persistency without having to allocate any extra memory. Additionally, if the given VMCS is the same as the one saved previously by the VMPTRLD instruction, then this information will be cleared as well.

VMREAD and VMWRITE instruction emulation require the blue pill software to create its own mapping from some VMCS field to some offset within the VMCS, allowing it to store and recall data from the VMCS structure. The VMCS pointer used for storing and recalling data is the one stored previously during the emulation of the VMPTRLD instruction. Some of Intel's newer CPUs support a feature called VMCS shadowing, which allows guest software to directly interact with some VMCS without requiring an exit from guest to host, making VMREAD and VMWRITE emulation easier.

VMRESUME and VMLAUNCH instructions emulation requires the blue pill software to create a shadow VMCS. The shadow VMCS is denoted as L_{02} VMCS, meaning it was created by level zero and describes a VM running at level two. The host state of L_{02} VMCS will describe the blue pill hypervisor instead of the one described by the red pill running on the guest. When an exit occurs from guest to host, it will first be to the blue pill hypervisor, and then, maybe, the red pill hypervisor will be executed if necessary. Thus, the time required to go from a guest executing at level 2 to level 1 by indirectly having to go through level 0. Therefore, it is impossible for the guest running at level 2 to have a similar performance of that running at level 1. Consequently, any red pill that can successfully detect a guest by timing and performance tests can easily expose a nested blue pill hypervisor by simply observing performance.

Multicore Red Pills

When discussing Pafish timing attacks, it has been shown how some x86 instructions can be used to perform timing attacks, i.e., they take a much longer time to operate when a hypervisor or red pill is present.

In an attempt to defeat these detection methods, a blue pill can take certain operations such as tampering with CPU time (RDTSC) instructions. Tampering with CPU timing can be used to change the CPU time measurements and build efficient rootkits.

However, there are other methods a core can use to measure time and CPU cycles.

Most modern CPUs include more than one core. All Intel's core iX processors include 4–36 cores. The extra cores (all cores beyond the first) can be used for time measurements. By performing certain operations in CPU registers (such as ADDing, ORing, or NOPing) a specific amount of time can be considered wasted and efficient time measurement can be provided even if the time measurement instructions (RDTSC) have been manipulated.

Undocumented Opcodes-Based Attacks

The x86 opcodes vary in length from 1 to 19 bytes. This massive address space leaves vast room for opcodes.

Domas (2017) mapped the opcodes and compared them with the x86 specs. Domas found many ($\sim 10^5$) undocumented opcodes in the x86 architecture. It is speculated that Intel's engineers use these instructions for internal testing. While the behaviour of these opcodes is undefined, by definition, it is not unlikely that by calling one of these opcodes one could generate a different behaviour if a red pill hypervisor is running. Further research on this subject is required.

SOLUTIONS AND RECOMMENDATIONS

As demonstrated above, there are numerous ways in which a hypervisor can hide and avoid detection and numerous ways in which a hypervisor can be detected. It is recommended to take the following precautions as a malicious blue pill must be avoided at all costs:

1. Install a TPM on the system and attest the UEFI BIOS.
2. Start an attested trusted hypervisor that will prevent any subversion attacks.
3. Update the applications or homegrown code if new subverting attacks are discovered and published (0-days).

If a red pill is required and a primordial hypervisor cannot be installed, then the recommended red pill method is to use remote attestation methods whenever possible.

Local attestation by the local system should be avoided, especially if the malicious hypervisor's designers can review the local attestation code and design the hypervisor so that it passes the local test with high probability.

However, if local attestation is required, then it is recommended to use the multiple cores available in all modern CPUs for time-based attestation. Such methods should be used as a last resort, and remote attestation or network timing-based methods are preferred. A malicious blue pill hypervisor can block these methods; however, tampering with NMIs between cores will usually introduce noticeable latency to the system.

It is also possible that unknown opcodes can be researched to provide new red pills.

FUTURE RESEARCH DIRECTIONS

Further research based on undocumented opcodes (Domas 2017) as described above is recommended. There are many unknown opcodes, and it is very likely that some of those opcodes behave differently in the presence of a hypervisor. Such opcodes may also behave differently in nested and ordinary virtualization.

If such instructions are found, then it will be challenging to overcome these red pill detections. The blue pill hypervisor may attempt to interpret each page loaded into memory and detect such instructions; however, because each instruction in x86 takes a variable number of bytes, detecting the offending instructions may force time-consuming tests of each memory page that gains execution permissions and, thus, may be detectable by other means.

Researching how the Kennell method can apply to new CPUs, especially generation 9 Intel CPUs with the new algorithms after spectre and meltdown attacks, is also an exciting research topic.

CONCLUSION

It was shown how modern blue pills and red pills could be constructed.

For constructing modern blue pills, the detection code must be available and analyzed.

It is quite possible that a given red pill (if analyzed by the blue pill coders) can be detected and bypassed; however, it is not possible to code a blue pill that will bypass all possible tests and still maintain proper system performance.

REFERENCES

- Averbuch, A., Kiperberg, M., & Zaidenberg, N. J. (2011, September). An efficient vm-based software protection. In *2011 5th International Conference on Network and System Security* (pp. 121-128). IEEE. 10.1109/ICNSS.2011.6059968
- Domas, C. (2017). *Breaking the x86 ISA*. Black Hat.
- Kennell, R., & Jamieson, L. H. (2003, August). Establishing the Genuinity of Remote Computer Systems. In *USENIX Security Symposium* (pp. 295-308). USENIX.
- Kennell, R., & Jamieson, L. H. (2004). An analysis of proposed attacks against genuinity tests. CERIAS, Purdue Univ.
- Kiperberg, M., & Zaidenberg, N. (2013). Efficient Remote Authentication. *Journal of Information Warfare*, 12(3), 49-55.
- Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., . . . Yarom, Y. (2018). *Spectre attacks: Exploiting speculative execution*. arXiv preprint arXiv:1801.01203
- Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., . . . Hamburg, M. (2018). *Meltdown*. arXiv preprint arXiv:1801.01207
- OrtegaA. (2016). *Paranoid Fish*. Retrieved from <https://github.com/aOrtega/pafish>
- Popek, G. J., & Goldberg, R. P. (1974). Formal requirements for virtualizable third generation architectures. *Communications of the ACM*, 17(7), 412-421. doi:10.1145/361011.361073
- Rutkowska, J. (2006). *Subverting Vista™ kernel for fun and profit*. Black Hat Briefings.
- Rutkowska, J., & Tereshkin, A. (2007). *IsGameOver () anyone*. Black Hat.
- Shankar, U., Chew, M., & Tygar, J. D. (2004, August). Side effects are not sufficient to authenticate software. In *USENIX Security Symposium (Vol. 8, No. 3)*. USENIX.
- Tarnovsky, C. (2010). Semiconductor security awareness today and yesterday. *Blackhat 2010*.
- Tarnovsky, C. (2012). Attacking tpm part two. *Defcon 2012*.
- Zaidenberg, N., Neittaanmäki, P., Kiperberg, M., & Resh, A. (2015). Trusted Computing and DRM. In *Cyber Security: Analytics, Technology and Automation* (pp. 205-212). Cham: Springer. doi:10.1007/978-3-319-18302-2_13

ADDITIONAL READING

Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., & Boneh, D. (2003, October). Terra: A virtual machine-based platform for trusted computing. *Operating Systems Review*, 37(5), 193–206. doi:10.1145/1165389.945464

Kauer, B. (2007, August). OSLO: Improving the Security of Trusted Computing. In *USENIX Security Symposium* (Vol. 24, p. 173).

Mitchell, C. (Ed.). (2005). Trusted computing (Vol. 6). Iet.

Resh, A., Kiperberg, M., Leon, R., & Zaidenberg, N. J. (2017). Preventing Execution of Unauthorized Native-Code Software. *International Journal of Digital Content Technology and its Applications*, 11.

Rutkowska, J. (2006). Introducing blue pill. *The official blog of the invisiblethings.org*, 22, 23.

Zaidenberg, N., & Resh, A. (2015). Timing and side channel attacks. In *Cyber Security: Analytics, Technology and Automation* (pp. 183–194). Cham: Springer. doi:10.1007/978-3-319-18302-2_11

Zaidenberg, N. J. (2018). Hardware Rooted Security in Industry 4.0 Systems. *Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures*, 51, 135

KEY TERMS AND DEFINITIONS

Blue Pill: Blue pill is a type of software that runs as a malicious thin hypervisor-based rootkit.

Bootkit: A rootkit that boots when the computer boots, usually before the operating system starts. The bootkit installs itself on the hard drive master boot record (MBR) or BIOS and gains control of the system before the operating system ever has control.

Chain of Trust: Group of computer components that starts at a trust nexus. Through a series of operations, each component in the chain adds functionality and verifies the next component. The final component is trusted if all components in the chain complete successful verification and then the nexus can indeed be trusted.

Hypervisor: A hypervisor is a type of computer software designed to run multiple operating systems on the same hardware.

Privilege Ring: Intel architecture defines several privilege “rings” (protection rings) that refer to the current state of the system. These rings are ring 3 (user mode) where certain operations are not allowed, ring 0 (supervisor mode/operating system mode) where access to hardware devices is allowed, and hypervisor mode (ring –1) where hypervisor operations are allowed. Rings 1 and 2 also exist: these “in-between” privilege levels had historical usage but are mainly unused in modern systems.

Red Pill: Red pill is a type of software that is used to detect and defeat blue pills. The goal of the red pill is to provide an answer to the question, “Is the computer currently running a blue pill?” in the most reliable possible method.

Rootkit: Rootkit is malicious software that grants unauthorized user-persistent access to the victim computer resources. The rootkit is also designed to mask its existence such that the administrator will not be able to detect it.

Thin Hypervisor: A hypervisor that is designed to support only one operating system.

Trusted Platform Module (TPM): The Trusted Platform Module (ISO/IEC 11889) is an international standard and specification for a secure cryptoprocessor. The TPM is a dedicated microcontroller designed with hardware obfuscation to prevent tampering. The TPM provides cryptographic operations and can measure the CPU and running software for platform attestation.

Arm Hypervisor and Trustzone Alternatives

Nezer Jacob Zaidenberg

College of Management, Israel

Raz Ben Yehuda

University of Jyväskylä, Finland

Roe Leon

University of Jyväskylä, Finland

INTRODUCTION

ARM holdings have proposed TrustZone™ as means to create a Trusted Execution Environment (TEE) on the ARM platform. On many scenarios, such Trust Execution Environment is required to provide DRM support, secure wallets, Trusted endpoints, point of sale and other embedded systems.

Other than the mobile platform, TrustZone™ can be found in other ARM socs, such as AMD with their “Hiero falcon”, AppleMicros X-Gene3, Cavium Thunder X etcetera.

Virtualization as a security solution is also widespread. Safe execution through sandboxing is a standard method for security. Several applications offer methods for trapping sensitive instructions into a hypervisor. Cloud computing technology, initially designed for dynamic provisioning of computing resources, is by its nature exposed to the public. Therefore, the virtual machine is exposed to many threats. Also, as the ARM architecture-based servers technology spreads, ARM virtualization technology can ease filtering out threats and monitor activities.

Multiple vendors offer their own TEE implementations. Some TEE implementations such as Trustonic and Qualcomm QSEE are closed source while others are open source or provide source code for a fee. This chapter surveys Trusted computing alternatives for implementations. The chapter mainly considers alternatives with available source code that offers a complete solution for the TrustZone™ environment, and also offers some ARM virtualization alternatives.

BACKGROUND

Trusted Execution Environment

The ARM architecture allows for co-existence of a Trusted Execution Environment (TEE) and Rich Execution Environment (REE). Trusted Execution Environment is a secure area inside the central processor unit (hereby CPU). The Trusted Execution Environment runs its own operating system. The TEE operating system is a separate operating system that is running in parallel with the REE(main) operating system, in an isolated environment. The Trusted Execution Environment guarantees that the code and data loaded in the TEE are protected concerning confidentiality and integrity.

DOI: 10.4018/978-1-5225-9715-5.ch079

Rich Execution Environment is another area inside the CPU. The Rich Execution Environment runs a separate operating system. Usually, Google's Android or Apple's iOS. The Rich Execution Environment refers to the standard operating system that the device is running. The Rich Execution Environment offers significantly more features and applications and as a result, is vulnerable to attacks. In most cases, the Rich Execution Environment is the environment where most applications are running. The Rich Execution Environment receive services such as decryption keys from the Trusted Execution Environment.

The Trusted Execution Environment usually act as a monitor for the Rich Execution Environment.

The Trusted Execution Environment has higher permissions and usually have access to read the Rich Execution Environment memory and data structures. The Rich Execution Environment should not have access to the trusted Execution environment memory and data structures. The two worlds, the secured and the normal (not trusted, non-secured) worlds, can switch through the strict supervision of a Secure Monitor running in monitor mode. Switching between the secure and normal world can be done through a special instruction called "secure monitor call" or SMC. Software use SMC to communicate between the secure and normal worlds shared memory is used. TrustZone™ splits the SOC devices to the secure and normal worlds. TrustZone™ control the device hardware interrupts. TrustZone™ can route an interrupt to the secure world or the normal world. Like in the memory case, I/O and interrupts routing may change dynamically. TrustZone™ uses its own MMU. Operating systems and processes that execute in TrustZone™ do not share the same address space with their normal world counterparts. Thus, there is no need to have distinct TrustZone™ for each processor. A single TrustZone™ OS across multiple ARM processors/cores can manage all the device Trusted computing needs. The cryptographic keys are accessible only in TrustZone™. The manufacturer can burn platform-specific keys using fuses. These platform-specific keys are device specific, thus enabling protection in the end unit level.

Booting a Trusted Execution Environment must form a chain of trust in which a trust nexus verifies the next component on the boot chain. Each component verifies the next component until the system. Many vendors proposed.

ARM Permission Model

ARMv8 architecture has a unique approach to privilege levels.

The ARM platform has 4 exception (permission) levels.

ARM also has the secure world (TrustZone™) and the normal world (non-TrustZone™)

ARM Exception levels are described in Table 1 Each of the exception levels provides its own set of registers and can access the registers of the lower exception levels but not registers of higher exception levels. The general-purpose registers are shared.

Thus, moving to a different exception level on the ARM architecture does not require the expensive context switch that is associated with the x86 architecture.

ARMv7 architecture is similar to ARMv8. ARMv7 offers virtualization as an extension that is only available to some late ARMv7 models. ARMv7 does offer TrustZone™. Furthermore, ARMv7 is 32bit architecture while ARMv8 is 64bit (and 32bit) architecture.

Virtualization vs TrustZone™ Mode

The first question we must address is how the operating system should be verified. The REE operating system can be verified using HYP mode or TrustZone™. ARM has designed the TrustZone™ mode specifically for attesting and monitoring the Rich operating system. Only the vendor can install soft-

Table 1. Arm exception levels

Exception level	Meaning	Notes
Exception Level 0 (EL0)	Refers to the userspace code.	EL0 exists in both the secure and the normal world. EL0 is analogous to x86 “ring 3”.
Exception Level 1 (EL1)	Refers to the operating system code.	EL1 exists in both the secure and the normal world. EL1 is analogous to x86 “ring 0”.
Exception Level 2 (EL2)	Refers to the HYP mode.	EL2 exists only in the normal world EL2 is analogous to x86 “ring -1”.
Exception Level 3 (EL3)	TrustZone™	Refers to TrustZone™ as a special security mode that can monitor the ARM processor and may run a real-time security OS. There is no direct analogous mode, but related concepts in x86 are Intel’s ME or SMM.

ware on the TrustZone™ mode. In some cases, even the vendor receives the CPU from a 3rd party and has limited access. In those cases, even the vendor cannot install any software in TrustZone™ mode. However, if not deliberately prohibited by the manufacturer, everybody can install any software in HYP mode. This usually makes hypervisor code easier to install. This chapter examines the problem from the vendor standpoint. Therefore it is assumed that TrustZone™ is available.

The two main drawbacks of using virtualization are that virtualization mode is no longer available for other software that may want to run there. Also, TrustZone™ is monitored on boot by the BSP (Board Support Package); it cannot be modified or replaced as easy as the hypervisor boot loader or driver.

Resh et al. (2017) and Seshadri et al. (2007) provide examples of using hypervisor for endpoint security.

We examine several hypervisor implementations for completion. However, it is assumed that a TrustZone™ solution is preferable whenever TrustZone™ is available.

Virtualization Classification

Virtualization is the process of running multiple Operating systems on a single hardware or running microkernel to manage a single operating system. A hypervisor is a software component that provides virtualization. There are two types of hypervisors:

1. Full virtualization - The guests’ operating systems are running as it would on regular hardware.

It is not modified in any way or aware of the fact that it does not run on bare-metal hardware.

2. Para-virtualization – The guest operating system is aware that it runs as a guest. The guest’s operating system code is modified. The guest operating system does not attempt to communicate directly with the hardware. Instead, the guest operating systems uses hypercalls to communicate with the host hypervisor. Hypercall is a call from the guest to the host. Similar to system call from a user process to the operating system. When the guest’s operating system needs the host, for example, for I/O access and sometimes in critical sections. The hypercall trap to the hypervisor to perform a service on behalf of the guest. As multiple guests are trying to access the same hardware, the hypervisor needs to trap and synchronize these access. Using para-virtualization and hypercalls usually yields better performance then trapping.

In the taxonomy of the virtualization environment, virtualization environments have two design categorize

1. Complete monolithic - A single software responsible for providing access to the hardware to the guests. For example, VMware ESXi server.
2. Partially monolithic - The technology is an extension to the general-purpose operating system, such as KVM in Linux and VMWare Desktop or Microsoft Hyper-V
3. MicroKernel These are lightweight microkernels that a minimal set of services to the guests, mainly CPU virtualization and hardware access. Jailhouse and seL4 are examples for such microvisors (micro hypervisors).

Last virtualization pioneers Popek and Goldberg (1974) classified hypervisors to type I and type II
Type I hypervisors (or boot hypervisors) – are hypervisors that start at boot and start various guest operating systems. Examples include VMWare ESXi, Xen and IBM S/390 VM.

Type II Hypervisors (or hosted hypervisors) – are hypervisors that starts under a host operating system that already booted and took control of the machine. Examples include VMWare desktop.

For security and trusted computing purposes, mainly Type I hypervisors are of interest. Type II hypervisors can be disabled by the host OS (for example malicious software can cancel the hypervisor start sequence after reboot) and thus type 2 hypervisors serve minimal security purpose.

GlobalPlatform

GlobalPlatform is a nonprofit organization that consists of an alliance of many mobile device manufacturers. GlobalPlatform creates and publishes the standard for secure digital services for mobile devices. GlobalPlatform (2011) is the current standard for TEE platform under ARM.

GENERAL DYNAMICS OKL4

OKL4 is a microkernel that was originally developed, maintained and distributed by Open Kernel Labs.

The OKL4 operating system was based on the L4 operating system by Liedtke (1996).

The L4 microkernels family in its earlier form was called L3. L3 was a microkernel that was developed Liedtke in the 1980s on an i386 system and was deployed in a few thousands' installations, mainly education institutes. L3 suffered from a high overhead of IPC communication, which was over 100us. Liedtke, trying to reduce the IPC overhead problem, had re-implemented L3 completely and reduced the IPC overhead significantly to 5us, on i486. This new design was referred to as L4.

L4 had evolved over the years and become a family of L4 microkernels, to name a few, L4-embedded, Codezero, NICTA, seL4 etcetera. NICTA was maintained by OpenLabs which renamed it to OKL4 microkernel and stopped the open source development.

OKL4 (Heiser et al. 2010) is deeply covered in peer-reviewed publications. The OKL4 micro-visor supports both para-virtualization and pure virtualization. It is designed for the IoT industry, and supports, ARMv5, ARMv6, ARMv7ve and ARM8va. OKL4 is focused on embedded devices. OKL4 was originally open source software.

On 2012 general dynamics acquired the Open Kernel Labs. After the acquisition, General Dynamics changed OKL4 source code policy from open to closed source project. The latest available open source

OKL4 is from May 2013 and is still available to download from archive.org (and other sources). OKL4 has a sister open source project (supported by GeneralDynamics) called seL4, which is described later.

Installing OKL4 and running it is a challenging task that requires expertise. Open source OKL4 code must also be adapted to modern hardware.

Today OKL4 is still under development and support of General Dynamics.

One can also obtain the current OKL4 source code under a suitable license and NDAs.

This chapter refers to the latest available open source OKL4 from 2013 and not to current releases, and thus this chapter is not up to date with current releases (compared to other Trusted Execution Environment alternatives) but does not violate any NDAs

GOOGLE TRUSTY TEE

Trusty is a secure Operating System (OS) that was developed by Google.

Trusty provides a Trusted Execution Environment (TEE) for The Android (only) Operating system.

The Trusty OS doesn't require security specific hardware. Instead, Trusty TEE runs on the same processor as the normal Android OS. However, despite running on the same CPU, Trusty is isolated from the rest of the system. This is done using ARM TrustZone™ features that enable separate MMU for trusty (in TrustZone™) and the normal world OS. TrustZone™ allows Trusty to create an isolated secure execution environment and provide certain services to the REE OS (i.e. Android).

Trusty consists of:

- A small operating system kernel. The Trusty kernel is derived from Little Kernel. Little Kernel is a small operating system that is also used as Android boot loader.
- A Linux kernel driver that acts as a mediator between the TEE (Trusty) and REE (Android) environments.
- An Android userspace library that provides a way to communicate between the REE (Android) and TEE (Trusty) applications using the kernel driver.

Trusty is compatible with ARM and Intel processors. On ARM systems, Trusty uses ARM's Trust-zone™ to virtualize the CPU and create a secure, trusted execution environment. Similar support is also available on Intel x86 platforms using Intel's Virtualization Technology.

LINARO OP-TEE

Linaro security working group and STMicroelectronics have teamed to create OP-TEE.

OP-TEE follows GlobalPlatform specification (2011) and implements version 1.1 of GlobalPlatform TEE client API and TEE internal API.

OP-TEE is an open source project and is widely available under BSD 2-clause license and (Kernel parts) GPLv2 license. OP-TEE has a small footprint and minimal effect on the running system. OP-TEE has vast community support.

Like Trusty above, OP-TEE consists of 3 main components.

- A lightweight, secure operating system. The OP-TEE operating system consists of several modules, such as memory management, interrupt handling, scheduler. Also, OP-TEE implements a hardware abstraction layer as it supports various processors and hardware. The OPTEE operating system also provides a capability to run user-space applications (typically referred to as Trustlets) in the secure world. These applications are provided with the GlobalPlatform TEE Internal API which allows them to ask for internal, secure-only, OS services
- A non-secure user-space client that is composed of two components: (1) a user-space/kernel-space mediator and (2) libraries that implement the GlobalPlatform TEE Client API.
- A kernel driver that performs the transitions between the secure and normal worlds

SOLUTIONS AND RECOMMENDATIONS

The features of the various TEE alternatives are shown in Table 2.

Table 2. Summarizes the TrustZone™ alternatives on ARM circa 2018

	OKL4	OP TEE	Trusty TEE
Vendor	General Dynamics since 2012, Originally Open Kernel Labs. (2006-2012)	Linaro	Google
Background	OKL4 Hypervisor designed by General Dynamics Mission Systems delivers a real-time embedded Type 1 virtualization solution using our proprietary OKL4 technology. Combined with Lightweight Execution Environments (LWEE) and proven commercial Linux, VxWorks or Android distributions, the OKL4 Hypervisor enables the ability to produce fully integrated, secure, and performance-optimized solutions with guaranteed separation. Applications, functions and processes running on separate dedicated operating systems and hardware can now be consolidated into one intelligent system, allowing for highly scalable and secure systems at a lower cost. ¹	OP-TEE is an Open Source TEE and is the result of collaboration work between STMicroelectronics and Linaro Security Working Group. It contains the complete stack from normal world client API's (optee_client), the Linux kernel TEE driver (optee_linuxdriver), the Trusted OS + the secure monitor (optee_os) and the test suite (xtest). ²	Trusty is a secure Operating System (OS) that provides a Trusted Execution Environment (TEE) for Android. The Trusty OS runs on the same processor as the Android OS, but Trusty is isolated from the rest of the system by both hardware and software. Trusty and Android run parallel to each other. Trusty has access to the full power of a device's CPU and memory but is completely isolated. Trusty's isolation protects it from malicious apps installed by the user and potential vulnerabilities that may be discovered in Android. ³
Source model	Open source until 2013. Currently closed source. Links to the older code base are still available. Current sources may be purchased from GD with some licenses and NDA restrictions. Current sources were not used in preparing this chapter.	Open source. BSD 2 clause and GPL (Kernel)	Open source Apache Open Source License and GPL. https://source.android.com/license
Link to sources	(2013 code base) http://web.archive.org/web/20130518095945/http://wiki.ok-labs.com/downloads/release-3.0/okl4_3.0.tar.gz	https://github.com/OP-TEE	https://android.googlesource.com/trusty
Scheduler	Thread scheduler	No scheduler. Scheduling is performed by the REE OS. Multi-process only. Multiple threads are not supported.	Round robin. Multi-process only. Multiple threads are not supported.
Memory management	hypervisor - OS isolation microkernel - cell isolation each run in non-privileged mode only microvisor run as privileged mode	Each TA instance is completely isolated.	Isolated processes under the Trusty TEE OS kernel. Each process runs in its own virtual memory sandbox utilizing the MMU capabilities of the TEE processor
Footprint	very very low	~240KB	Not very big but larger than OP-TEE

continues on following page

Table 2. Continued

	OKL4	OP TEE	Trusty TEE
Maintenance level	Open source (2016) is not supported. Support can be purchased from GD	Maintained by Linaro and the community 10 releases (from which 6 release candidates) since 01.2018	Maintained and supported by Google. No active volunteer developer community. (Google employees develop Trusty)
Toolchain support	Proprietary API and tools by Open Kernel Labs/GD	OP-Tee follows global platform API reference	Google provides Trusty API reference at https://source.android.com/security/trusty/trusty-ref
Hardware support	ARM8, ARM7, ARM6	ARMv7, ARMv8	ARMv8, ARMv7 and Intel (Using Intel VT-x)
Secure to normal world interface. Ease of Development on normal world	Proprietary API	ioctl	IOCTL / using port
Logging support	Multiple mechanisms exist	Configurable Log level (such as in Linux). Several macros DMSG/EMSG/IMSG/ FMSG may be used and redirected to UART	standard output. Data written to standard output can be routed (depending on the LK debug level) to UART or a memory log available on the non-secure side, depending on the platform and configuration. Non-critical debug logs and messages should go in standard output. The read() and ioctl() methods are no-ops and should return an ERR_NOT_SUPPORTED error.
Power up delay	Not noticeable	Not noticeable	Not noticeable

OTHER ALTERNATIVES

These alternatives are not as strong as the alternatives mentioned above

Jailhouse

Announced by Siemens at November 2013, Jailhouse (Baryshnikov 2016) is a type 2 partitioning microvisor for Linux hosts. A partitioning microvisor is a microvisor that controls access to resources and isolates them from the general-purpose operating system - GPOS or other guests. Partitioning means a strict allocation of the system resources. The hosting Linux is referred to as the “Root cell”, and the guests are “inmates”. Jailhouse is not an operating system; it a resource access controller. Jailhouse is controlled from the Linux host, which makes it reveals to hosting Linux, but not the guest.

Jailhouse is a bare-metal hypervisor, and in most cases, it is pure virtualization hypervisor, and as such can run many types of operating systems, such as FreeRTOS, Erika3, Linux and Zephyr. It supports ARMv8, ARMv7a, and x86_64. Jailhouse requires the machine to have at least two processors. One processor is used to run the hosting Linux, and the other processors may be assigned to Jailhouse. It requires the Linux kernel to reserve a contiguous memory at boot time. It requires a memory footprint of a few tens of megabytes, usually 50 megabytes.

The configuration of Jailhouse is done through a tool provided by Jailhouse. This tool scan sysfs and procfs, and then generates a device tree that describes the hardware as seen by the Linux host. This device tree is referred to as the cell configuration file. It is up to the user to edit the cell file to create a correct guest configuration. It is a process of trial and error.

Jailhouse targets the automation, robotics and IoT industries.

QSEE

QSEE is Qualcomm Secure Execution Environment. In the past, it was based on OKL4 until GeneralDynamics and Qualcomm failed to reach an agreement regarding licensing. Since 2015-6 Qualcomm has developed QSEE from scratch with no (direct) connection to GeneralDynamics.

QSEE is closed source (and Qualcomm does not provide source code licenses) Therefore, QSEE fails this chapter precondition of source availability and is not part of this survey.

Prior releases of QSEE suffered from several well-documented security problems.

seL4

seL4 like OKL4 is also based on the L4 microkernel. seL4 (Klein et al. 2009) is a microvisor that was implemented by Open Kernels labs (and later GeneralDynamics). seL4 is not as popular as OKL4. One of the powerful features of seL4 is the fact that it has been formally verified to be correct.

seL4 compared to OKL4, is an open source kernel. seL4 is the sole kernel that is mathematically proven secure and safe. L4-embedded, or NICTA embedded, was adopted by Qualcomm as a real-time operating system for their wireless modem processors firmware.

The basic rules of the L4 kernel design are minimalism. Leidtke (1996) formulated the rule of minimization as follows:

“A concept is tolerated inside the u-microkernel only if moving it outside the kernel, i.e. permitting competing implementation would prevent the implementation of system required functionality”.

This principle, also known as the no-policy in the kernel, is the core of the L4 microkernels design. Though operating systems tend to grow in size over the years, L4 footprint is considerably low. The seL4 footprint is 9600 lines of code. As a side effect of the minimization and performance, L4 microkernels do not strive to hardware abstraction. Half of the seL4 microkernel is agnostic to the underlying hardware.

L4 also demonstrates a new resource management scheme where all memory allocations are userspace driven. Another interesting feature of the L4 microkernels is the fact that interrupts are disabled while executing in kernel mode. This approach simplifies the implementation, increases the performance and eases the kernel verification. Direct process switch, which in general means that seL4 tries to avoid using the scheduler, is another exciting facet of L4. When a thread reaches a preemption point, the kernel switches to the first runnable thread, which in turn, executes on the time slice of the preempted thread.

seL4 runs on ARM, supports SMP and Uniprocessor. seL4 also provides real-time support.

TrustTonic

TrustTonic is a company known for its TrustZone technology in the mobile world, mainly Android. The TrustTonic operating system, Kinibi, is a closed source operating system. The Kinibi OS is widespread in the Android cellphone world. Kinibi provides data encryption and device authentication features. Kinibi also gives safe access to peripherals, such as the touch screen, NFC and fingerprint, through its TEE API, so that no malware in the REE can access secure communication and data. In addition, Kinibi can isolate sensitive code execution and secure data.

The secure boot chain of trust verifies kinibi, i.e. it is verified by the bootloader each time the device boots.

Above all that, Kinibi TEE applications has access to the network. This way, a trusted application can access remote services securely.

TrustTonic can also be found in the automotive industry. In this area, TrustTonic approaches data leakage, application overlapping and application re-packaging attacks. Application overlapping attack is an interception technique for stealing sensitive I/O, such as when a user enters its password. A repacking of an application is a method of modifying a program to steal sensitive data. For example, adding a log entry that prints sensitive information.

Trustonic offers an SDK, compliant with GlobalPlatform API standards, to help build Trusted Applications.

Xen

Announced at 2003 and developed initially at the University of Cambridge, by Ian Pratt, Xen is a hypervisor. Xen provides CPU virtualization Virtual interrupts, virtual MMU and inter-guest communication. In Xen, a virtual machine is referred to as Domain. Domain0, also known as Dom0, is the first domain that must run before any other virtual machine and it is usually Linux or BSD, and DomU is a virtual machine on top of the other domains. Domain0 requires access to the entire machine's hardware. Domain0 responsibility is managed through the Linux kernel. Xen's event channel provides communication between Dom0 and DomU. Whenever DomU issues a virtualized event, it uses this event channel. The event channel is used for para-virtualized guests. For a full virtualized guest, Xen uses QEMU. Xen's tool stack is the management tool to control guests. The fact that Xen uses Linux as Dom0 provides Xen with an abundant of hardware support and Linux software. Xen boots from the bootloader and is then loads the para-virtualized host.

This comes with some cost of performance. Virtualized I/O accesses and virtualized interrupts are routed from DomU Xen guests are delegated to Dom0. In addition, if a host interrupt occurs while DomU runs, then this interrupt would be served only when Dom0 is getting the processor. Thus, interrupts and events have an overhead.

Xen is available in ARM and x86, runs on SMP and UP. Xen is licensed GPL.

Xvisor

Announced at Apr 2012, Xvisor (Patal et al. 2015), is a monolithic, type 1 hypervisor independent of Linux. A monolithic hypervisor controls the hardware peripherals. Xvisor provides a minimal operating system, and it is not a microkernel. Xvisor can emulate devices and provides a path-through access to real devices. As an operating system, it has a memory management, scheduler, load balancer and threads. There are no processes in Xvisor. Furthermore, Xvisor is not POSIX compliant. Xvisor support SMP, so that a guest can use two or more processors. There are no restrictions on the number of processors, and Xvisor can execute on a single processor.

Xvisor provides an IPC between two guests through the use of an aliased guest region, which is a GPA (guest physical address) shared between two guests. In the Xvisor taxonomy, a processor can be Normal VCPU or an Orphan VCPU.

Normal VCPUs serve guests OSes, and Orphan VCPUs belongs to the hypervisor. Xvisor support ARM 32bit and 64bit and x86. Its footprint is less than 10MB, however, since it is a type 1 hypervisor, it is required to change the boot loader. Xvisor targets the infotainment market in the automobile world and automation in general. It is licensed GPL.

FUTURE RESEARCH DIRECTIONS

Research on ARM TEE is ongoing and proceeds in several fronts.

First and foremost, the current implementation and chain of trust are examined. Multiple errors and bugs are found and reported, and ongoing research is carried over to locate bugs in current versions of ARM TEEs. This research is carried over by ethical hackers trying to perfect the current TEE platforms and also by attackers who try to exploit weaknesses and elevate permissions on current ARM TEEs.

A new research direction is trying to globalize TEE API for ARM, Intel, AMD and other architecture. Creating cross platform TEE environment can provide benefits to application authors.

Such extensions can be completed by using platform-specific APIs such as Intel's SGX (Secure Guard Extensions) to provide platform independent code.

Last TrustZone™ and other extensions can be used for other means such as real-time processing (Ben Yehuda et al. 2018) and Control flow analysis (Abera et al. 2016). Using the TrustZone™ architecture for other purposes is another interesting research area.

CONCLUSION

This chapter surveyed the popular TEE alternatives available today. Each alternative has its own benefits. SoC vendors and Platform manufacturers can choose the desired implementation based on their requirements and preferences.

We found that for many applications the free, open source, community driven OP-TEE offers equivalent or even better features even when compared to commercial alternatives or alternatives backed by massive companies.

REFERENCES

- Abera, T., Asokan, N., Davi, L., Ekberg, J. E., Nyman, T., Paverd, A., ... Tsudik, G. (2016, October). C-FLAT: control-flow attestation for embedded systems software. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 743-754). ACM. 10.1145/2976749.2978358
- ARM. (2009). *Security technology building a secure system using TrustZone™ technology* (white paper). ARM Limited.
- Baryshnikov, M. (2016). *Jailhouse hypervisor* (Bachelor's thesis). České vysoké učení technické v Praze. Vypočetní a informační centrum.
- Bech, J. (2014). *OP-TEE, open-source security for the mass-market*. Core Dump.

- Ben Yehuda, R., & Zaidenberg, N. J. (2018). Hyplets - Multi Exception Level Kernel towards Linux RTOS. *Proceedings of the 11th ACM International Systems and Storage Conference Systor 2018*, 116–117.
- Heiser, G., & Leslie, B. (2010, August). The OKL4 Microvisor: Convergence point of microkernels and hypervisors. In *Proceedings of the first ACM Asia-pacific workshop on Workshop on systems* (pp. 19–24). ACM. 10.1145/1851276.1851282
- Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., ... Sewell, T. (2009, October). seL4: Formal verification of an OS kernel. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles* (pp. 207–220). ACM. 10.1145/1629575.1629596
- Liedtke, J. (1996). Toward real microkernels. *Communications of the ACM*, 39(9), 70–77. doi:10.1145/234215.234473
- Patel, A., Daftedar, M., Shalan, M., & El-Kharashi, M. W. (2015, March). Embedded hypervisor xvisor: A comparative analysis. In *Parallel, Distributed and Network-Based Processing (PDP), 2015 23rd Euromicro International Conference on* (pp. 682–691). IEEE. 10.1109/PDP.2015.108
- Popek, G. J., & Goldberg, R. P. (1974). Formal requirements for virtualizable third generation architectures. *Communications of the ACM*, 17(7), 412–421. doi:10.1145/361011.361073
- Resh, A., Kiperberg, M., Leon, R., & Zaidenberg, N. J. (2017). Preventing Execution of Unauthorized Native-Code Software. *International Journal of Digital Content Technology and its Applications*, 11.
- Zaidenberg, N. J. (2018). Hardware Rooted Security in Industry 4.0 Systems. *Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures*, 51, 135–151.

ADDITIONAL READING

- Ekberg, J. E., Kostiainen, K., & Asokan, N. (2014). The untapped potential of trusted execution environments on mobile devices. *IEEE Security and Privacy*, 12(4), 29–37. doi:10.1109/MSP.2014.38
- GlobalPlatform Specification, (2011). TEE System Architecture, version 1.0.
- Seshadri, A., Luk, M., Qu, N., & Perrig, A. (2007, October). SecVisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity OSes. *Operating Systems Review*, 41(6), 335–350. doi:10.1145/1323293.1294294
- Shepherd, C., Arfaoui, G., Gurulian, I., Lee, R. P., Markantonakis, K., Akram, R. N., . . . Conchon, E. (2016, August). Secure and trusted execution: Past, present, and future-a critical review in the context of the internet of things and cyber-physical systems. In *Trustcom/BigDataSE/I SPA, 2016 IEEE* (pp. 168–177). IEEE.
- Zaidenberg, N., Neittaanmäki, P., Kiperberg, M., & Resh, A. (2015). Trusted Computing and DRM. In *Cyber Security: Analytics, Technology and Automation* (pp. 205–212). Cham: Springer. doi:10.1007/978-3-319-18302-2_13

KEY TERMS AND DEFINITIONS

ARM Architecture: ARM (previously advanced RISC machine, Acron RISC machine) is a 32 or 64 bit RISC CPU architecture that is by far the most common architecture in use today in mobile devices and IoT. ARM architecture includes TrustZone™ since the 7th generation of the ARM architecture.

ARM Virtualization: ARM offered virtualization extensions to ARM7 architecture and virtualization instructions as part of ARM8 architecture.

Board Support Package (BSP): A minimal set of drivers and boot loader to boot the operating system.

Chain of Trust: Group of computer components that starts at a trust nexus. Through a series of operations, each component in the chain adds functionality and verifies the next component. The final component is trusted if all components in the chain complete successful verification and then the nexus can indeed be trusted.

GlobalPlatform: Is an organization that publishes the standard for secure mobile and embedded platform

Hypercall: The term is analogous to System call. A call by a user process or the operating system for the hypervisor to perform some service required by the operating system of process.

Hypervisor: The hypervisor is the software component that is responsible for running multiple operating systems on the same hardware.

L4: A family of microkernel operating systems by Liedtke initially. OKL4 and seL4 are operating systems that were derived from L4.

Normal World (Insecure World): The normal operating system that the given platform is running for normal applications. In most cases, this refers to Google's Android or Apple's iOS.

Rich Execution Environment (REE): Rich Execution Environment is another area inside the main processor. The Rich Execution Environment runs a separate operating system. Usually, Google's Android or Apple's iOS. The Rich Execution Environment refers to the standard operating system that the device is running. The Rich Execution Environment offers significantly more features and applications and as a result, is vulnerable to attacks.

Secure World: Secure world is the name for the secure, trusted execution environment (TEE) on ARM Architecture. It is running concurrently, on the same CPU as the normal world. However, ARM provides hardware and software mechanisms to ensure that the normal world and secure worlds are running on separate environments.

Trusted Execution Environment (TEE): A Trusted Execution Environment (TEE) is a secure area inside the main processor. The trusted execution environment runs a separate operating system in parallel to the main operating system in an isolated environment. The trusted execution environment guarantees the confidentiality and integrity of the code and data loaded in the TEE.

TrustZone™: An ARM Exception level that allows running TEE in a secure environment in parallel to the normal ARM environment.

ENDNOTES

- ¹ As defined in “OKL4 Hypervisor Real-Time Embedded Type 1 Virtualization Solution” <https://gdmissionsystems.com/-/media/General-Dynamics/Cyber-and-Electronic-Warfare-Systems/PDF/Data-Sheets/okl4-hypervisor-datasheet.ashx?la=en&hash=50D69D27DFB3EDA4EA8C59928552848D01C9319D>
- ² As defined in <https://wiki.linaro.org/WorkingGroups/Security/OP-TEE>
- ³ As defined in <https://source.android.com/security/trusty>

Glossary

Academic Cheating: An individual who does not utilize their own intelligence to give their interpretation of the content.

Activism: A strategy implementing a form of forceful demonstration in order to bring about partisan or societal transformation.

Addiction or Addictive Behaviour: Actions which a person can no longer control. Someone may go online to send an e-mail, get distracted and remain online for several hours, and possibly forget to send the e-mail.

Alternative Media Outlets: In Singapore, this refers to platforms which are not under the ownership of Singapore's mainstream media organisations: Mediacorp and Singapore Press Holdings. These sites predominantly accept posts from contributors who may be anonymous.

AMNSTE: An acronym for a research tool developed by the authors during the on-going research project, Affiliate Marketing Network Simulation and Testing Environment, which has been previously published.

Anonymity: Anonymity and thus anonymous data is any information from which the person to whom the data relates cannot be identified, whether by the company processing the data or by any other person.

Anonymization: A process of destroying on-line tracks of the data that could be used to link it to its originator.

Anxiety: A mental health disorder which includes symptoms of worry, anxiety, and/or fear that are intense enough to disrupt one's daily activities.

API: Application programming interface, a set of subroutine definitions, communication protocols, and tools for building software.

Approach: LCT step used more by contact-driven offenders to facilitate in-person meeting.

ARM Architecture: ARM (previously advanced RISC machine, Acron RISC machine) is a 32 or 64 bit RISC CPU architecture that is by far the most common architecture in use today in mobile devices and IoT. ARM architecture includes TrustZone™ since the 7th generation of the ARM architecture.

ARM Virtualization: ARM offered virtualization extensions to ARM7 architecture and virtualization instructions as part of ARM8 architecture.

Article Scraping: It is a process of scraping of the articles from the blogs or websites.

Artificial Intelligence (AI): A multidisciplinary field of research and engineering which studies the human functions that can be emulated by different types of machines.

Audit and Policy Mechanisms: Is a section of avatar-based management techniques.

Auditing: The process of conducting an official inspection of a company or its accounts.

Authentication: Permission to access something, which is confidential. The authentication is only provided to authentic users.

Avatar-Based Management: Is control methods and techniques introduced by V. Mkrttchian in 2018.

Axial Coding: The process of identifying the relationships between the categories and linking them together. The process yields subcategories that are grouped under a specific category. This process takes place after open coding.

Big Data: A data set this is too large for “standard” software programs, and is generally used to identify large trends, and predict behaviors and outcomes.

Bitcoin: A digital cryptocurrency that is used for transactions in many black markets of the dark web. Invented in 2008 by Satoshi Nakamoto to create a decentralized digital currency used to record peer-to-peer transactions generated by complicated mathematical models to ensure security without the need for intermediaries such as central banks.

Block Chain: A list of records, called blocks, which are linked using cryptography and used as a ledger mechanism in cryptocurrency. Each block contains a cryptographic hash of the previous block a timestamp, and transaction data.

Blue Pill: Blue pill is a type of software that runs as a malicious thin hypervisor-based rootkit.

Board Support Package (BSP): A minimal set of drivers and boot loader to boot the operating system.

Boot Loader: A small piece of code that provides minimal functions. The boot loader is executed prior to booting the operating system. The boot loader typically provides minimal hardware drivers, file system support etc. that are required for reading the operating system code.

Bootkit: A rootkit that boots when the computer boots, usually before the operating system starts. The bootkit installs itself on the hard drive master boot record (MBR) or BIOS and gains control of the system before the operating system ever has control.

Bot: It is a virtual robot created to automotive task both simple and repetitive.

Botmaster: Botmaster is the master of bots on the network. A botmaster is responsible for keeping the bot online, sending control commands to bots for its operation, making sure to fix issues with bots, and set a set of rules for bots to function.

Botnet: A botnet is a collection of bots. Botnets originate many types of attacks like distributed denial-of-service attack (DDoS attack), data theft, spamming, and intrusion to systems and networks.

Bots: Any system connected to Internet becomes a bot when it runs automated tasks or scripts over the internet. Majority of the malicious web traffic gets originated from bots.

Brightfield: All criminal cases in a particular area known to the authorities.

Bullying: Arrogant attitude of people who oppress their peers through acts of physical and verbal violence. It is diffused mostly in scholar and juvenile contexts.

C&C Server: A command and control server (C&C server) is a system that issues directives to other connected systems that have been infected with rootkits or other types of malware, such as ransomware.

CAPTCHA: Completely automated public Turing test to state computers and humans separately is a technique implemented in some banking systems whose aim is to render bots by creating and rating tests that humans can clear but existing computer programs cannot.

Cashless Policy: A policy that discourages the use of huge raw cash for transactions but encourages the use of bank transfer, ATM card, POS, and other financial instruments for transferring cash in transactions.

Catfishing: Using digital tools and techniques to post false information, profiles, and or photographs with the sole purpose of intentionally manipulating, misleading, or harming others.

Certificate Transparency: Google's certificate transparency project repairs several structural defects in the SSL certificate system, which is the key cryptographic system that triggers all HTTPS connections.

Chain of Trust: Group of computer components that starts at a trust nexus. Through a series of operations, each component in the chain adds functionality and verifies the next component. The final component is trusted if all components in the chain complete successful verification and then the nexus can indeed be trusted.

Child Pornography: Any visual depiction of sexually explicit conduct involving a minor.

Child Prostitution: A youth involved in sexual activity for profit, whether financial or otherwise.

Child Sex Tourism: The commercial sexual exploitation of children by people who travel from one location to another and take part in sexual acts with children.

Child Sex Trafficking: The recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a minor for the purpose of a commercial sex act.

Cleynet: Mainstream websites that are indexed by popular search engines, like Yandex, Google, and Bing.

Click Spam: It is a process of executing clicks on behalf of user without the knowledge of user.

Clickbait: Web article with an attention-gathering headline designed to make users click on the link, but with content rarely connected to the headline at all.

Cloaking: It is a process of providing different versions of a page to the crawlers.

Cloning: Creating a replica of websites or cards with intent to defraud.

Cloud Act: Cloud Act is the U.S. legislation related to the transfer of electronic data with provisions for obtaining data for evidence and prosecution and also regulating transfer for foreign governments.

Cloud Computing: A type of computing that relies on shared computing resources rather than having local servers or personal devices to handle applications.

CNI: Critical national infrastructure.

Cold War: Intense bipolar international competition for influence and control between the United States and the Union of Soviet Socialist Republics (USSR). It began at the close of the Second World War and continuing until Soviet-installed communist regimes collapsed in Eastern Europe in 1989 and the USSR itself disintegrated in 1991. This conflict was labelled cold because nuclear weapons made direct military combat between the two likely to result in mutual suicide through escalation to so-called mutual assured destruction. The US and the USSR and their allies and clients therefore competed indirectly through competitive interference in the internal politics of third actors. The Cold War established the template for international conflict between nuclear powers. The cause of US and Soviet conflict is still debated; some argue it was due to mutual fear, others argue that one or the other was bent on imperial expansion, and still others argue that both were bent on imperial expansion. The politically prevailing view in the US today is that the US prevailed over the Soviet Union in the Cold War. Consequently, American-dominated Cold War-formed institutions such as NATO are positive tools for international stability and peace. They should be expanded and adapted to changed circumstances.

Collapsology: A set of theories that assume Western societies are about to collapse, and that the global crisis is imminent.

Collectivism: A cultural value that stressed the importance of the group over individual goals and cohesion within social groups.

Commerical Cyberstalker: A perpetrator who engage in cyberstalking for the purpose of financial gain.

Computer Fraud and Abuse Act: This 1986 Act serves as a modification to existing laws seeking to address issues of deception within the cyber realm. Computer users must receive proper authorization and must not exceed boundaries of authorization.

Congress: A national legislative body, especially that of the US. The US Congress, which meets at the Capitol in Washington DC, was established by the Constitution of 1787. It is composed of the Senate and the House of Representatives.

Console: An entertainment system designed to play video games (e.g., Microsoft's Xbox or Sony's PlayStation).

Contact-Driven Offender: Online sexual offenders who seek face-to-face contact with their child victims to engage in physical sexual activity (Briggs et al., 2011).

Content Scraping: It is a process of lifting off the displayed content from various websites and using it somewhere else or displaying it on other websites.

Conversational Analysis: Study of the frame of the conversation with specific attention paid to interactive details (interruptions, reformulations).

Conversion: A visitor to an e-commerce site completes a desired monetary transaction such as buying product or signing up for a service or a membership or whatever expectations an e-commerce site is intended to achieve by having visitors to the e-commerce site. A visit converts to a monetary outcome.

Convolutional Neural Networks (CNN): A special type of neural networks used popularly to analyze photography and imagery.

Cookies: Small text files that are placed on a user's web browser as they visit a website.

Covert Communication: Communication through methods that are designed to make such communication undetectable or unsuspecting.

CPA: Cost-per-acquisition advertising model pays affiliates only for visitor traffic that generated an income for the e-commerce site.

CPC: Cost-per-click advertising model pays affiliates for each visitor that was re-directed to the advertiser's e-commerce site, immaterial of the financial outcome; even if the visitor does not buy any products.

CPM: Cost-per-mille advertising model pays affiliates for simply displaying an advertisement of the e-commerce site to a visitor to the affiliate's website. This model requires least interaction by a visitor.

Crawling: It is the process by which search engines gather online information through crawling robots by moving from one web page to another by the use of hyperlinks.

Crime: Any illegal action that is considered an offence and is punishable by law.

Crime-Fake News: Fake news content which commits a transgression within the legal system in Singapore that can warrant a fine, imprisonment, or both.

Criminal Justice System: A system inclusive of law enforcement, the courts, and correctional practices established to control crime and penalize violators.

Criminal Negligence: Reckless disregard for the lives or safety of other persons. In health care contexts, healthcare providers have a fiduciary responsibility for providing appropriate treatment to patients under their care. Many nations have laws that make overt negligence in the provision of healthcare a criminal offence.

Criminology: The critical and systematic examination of how laws are made, the means, modes and motives of criminal offenders, and the collaborative responses to criminal activities by the judicial system, policy makers and community stakeholders.

Critical Discourse Analysis: Field of research that compares the social role of the speakers and the scene of enunciation.

Cross-Site Scripting (XSS): Injecting malicious code to be displayed in the victim's web browser to steal the victim's credentials.

Crowdsourcing: The practice of hiring a (large) group of people (the 'crowd') to accomplish a certain task, usually a repetitive task that does not require special training but that must be carried out over a large amount of data.

Cryptocurrency: A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Cryptography: A strategy for encoding data in a specific way with the goal that those for whom it is planned can peruse and process it.

Cryptology: A technique used to secure communicating of information, data and messages by implementing special protocols and algorithms aims to prevent other parties from reading and understanding the information transmitted.

Cryptomarkets: A cryptomarket may be defined as a platform for exchange of goods and services, both legal and illegal, on the dark web. They remain hidden from the world due to the use of anonymizing browsers such as TOR based on encryption techniques. Majority of the cryptomarkets undertake the sale and purchase of drugs.

Cyber: A broad term relating to or characteristic of the culture involving computers, information technology, and the internet.

Cyber Abuse: Online behavior that threatens, intimidate, harass, harm, or humiliate a person.

Cyber Hygiene: Cyber protective behaviours that people engage in whilst on the computer and internet, such as installing and updating anti-virus software.

Cyber Law: The legal system dealing with cyberspace and the internet.

Cyber Security: The section of information security, within the framework of which the processes of formation, functioning and evolution of cyber objects are studied, to identify sources of cyber-danger formed while determining their characteristics, as well as their classification and formation of regulatory documents, implementation of security systems in future.

Cyber Security Skills: Cyber security skills are those skills associated with ensuring the security of information technology (IT-generally referring to information storage and integrity) and operational technology (OT-referring to systems that control physical devices).

Cyber Sovereignty: This is a phrase commonly used in the field of internet governance to define the will of states to exercise and sustain control over the Internet domain within their own borders, including political, economic, cultural and technological activities. However, it is not clear how to apply this sovereignty concept to current international relations and international laws.

Cyber-Victimization: Cyber-victimization refers to the process in which others are victimized through the use of information and communication technologies.

Cyber-Vulnerabilities: A flaw in a computer system that can make the system vulnerable to attack. A cyber-vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Cyberattack: A malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.

Cyberbully: A person who directly or indirectly uses technology to reduce another person to a psychologically inferior state.

Cyberbullying: The act of bullying by using tools available on electronic devices which connect to the internet, messaging services, and others digital communication networks.

Cybercrime: The usage of the computer and its related technologies for the purpose of disrupting, with the motivation to gain financial gains or causing political, social, and psychological harm.

Cybercrime Legislation: The process of making laws regulating cybercrime.

Cybercriminals: Individuals who commit crimes via the internet.

Cybersafety: Is the safe and responsible use of Information and Communication Technologies (ICT). NetSafe's approach to cybersafety is founded on: Maintaining a positive approach about the many benefits brought by technologies. Encouraging the public to identify the risks associated with ICT.

Cyberspace: Cyberspace is the environment created by the tangible links (computers), intangible (application and services), and networks (internet and telecommunication).

Cyberstalking: A form of harassment where the cyberbully makes continuous threats and sends inappropriate messages to an individual in the form of text messages, instant messaging, social media, emails.

Cyberterrorism: The use of information and communication technology to cause grave disruption or pervasive fear.

Cyberwarfare: Cyberwarfare is an overt or covert action of states, non-state actors or state-backed attackers that includes various tactics and techniques, notably advanced persistent threats, phishing tactics, viruses like Stuxnet, botnets, Trojan horses, zombies, Metasploit, SQL attacks, Rootkit, Nessus, pharming, Wireshark and buffer overflows to target infrastructure, software systems, and governmental institutions of different parties.

Cyberworld: The world of inter-computer communication.

DAO: Is an organization represented by rules encoded as a computer program that is transparent, controlled by shareholders and not influenced by a central government.

Dapps: Decentralized applications (dApps) are applications that run on a P2P network of computers rather than a single computer.

Dark Web: A small part of the deep web that has been intentionally hidden and is inaccessible through ordinary web browsers. It is accessible through using specialized software to hide the internet protocol (IP) address to provide absolute anonymity to users. The dark web has become a haven for criminal activity.

Darkfield: All criminal cases, in a certain area, that are not known to the authorities.

Darknet: The hidden computer network typically used for illegal trading and forums to include illicit activities such as human trafficking.

Data Breach: A security incident involving unauthorized access to data.

Data Execution Prevention (DEP or W^X): A paradigm that dictates that memory pages can have either execute or write permission but not both. Data execution prevention prevents self-modifying code and also attacks on the code that runs by itself (by exploiting buffer overflows and similar attack forcing the code to rewrite itself). DEP is a critical feature in almost all modern operating systems.

Data Scraping: It is a process used to extract massive amount of data from websites in which the data is stored in local computer system or in structured database.

DDR: Disarmament, demobilisation, and reintegration.

Decipherment: The inverse of encipherment which is also an algorithm to change unreadable messages to readable messages.

Deep Web: The part of the web not a part of the surface web. It includes content inaccessible through the use of a search engine. These include private servers that only those with permission may access, intranets utilized by a variety of organizations, or even typical social media pages that users wish to keep concealed from the general public.

Denial of Service Attack (DDoS): The activities which disrupt the services of the computer rendering the computer usage ineffective for the user.

Developed Country: A self-governing country with advanced technological infrastructure, a developed economy as well as an advanced industry.

Developing Country: A country that is still seeking to become advanced in all spheres that is industrially, economically, politically, and socially.

Digital Age: The period in which smart machines are determinative in social life.

Digital Cage: Refers to an opinion that every moment of the lives of individuals is under surveillance in the digital age.

Digital Evidence: Information that is stored and transmitted on digital devices.

Digital Millennium Copyright Act (DMCA): A united state law that defines what constitute of fair use by the end-user and what constitutes as piracy or DRM violation. The DMCA criminalizes production of devices whose sole perhaps is breaking DRM.

Digital Psychology: It is a multidisciplinary (Behavioral Economics, Psychology, Digital Communication, and Information Technology) approach to psychology which integrates the study of human beings with the research on new technologies.

Digital Rights Management (DRM): A software subsystem designed to allow rightful users to use contents (games, media) they paid for and disallow illegal use of contents the user has not paid for. DRM is mainly designed to limit the end-user, and as such, DRM software is not liked by the users.

Digital Signature: A secure mathematical algorithm used to validate the credentials of digital documents and coded information associated with pre-approved signer to approve transactions.

Disclosure: The process of revealing something.

Discursive Ethos: Image of the self that appears during an interview or a discussion.

Disidentification: The disappearance of an individuals' real social identifications in the digital world.

Disinformation: False content that is deliberately fabricated and distributed.

DNS Pharming: Providing a fraudulent DNS mapping to direct a victim to visit a fake and malicious website.

Domain-Specific Search (DSS): The problem of building a (rudimentary or advanced) search engine over a domain-specific corpus. Domains of special interest in this article were illicit domains such as human trafficking, over which building such an engine is an especially challenging problem.

Drugs: A drug can be defined as any substance, chemical or natural, that is consumed for purposes other than medicinal and scientific.

E-Fencing: Selling stolen property on electronic platforms to make it look like normal electronic commerce.

Economic Growth: It can be defined as the increase in the capability of an economy to produce goods and services from one period to another. It can be measured either in nominal terms or in inflation adjusted real terms. Typically, GDP or GNP is taken as a measure of economic growth. In notational terms, GDP growth rate, g_t , AU54: Mathtype 7 where, t indicates the particular time point.

Elliptic Curve: A curve in two dimensions, which is known by its group property on points. It is widely used in cryptography due to its hard assumptions.

Elliptic Curves Digital Signature Algorithm (ECDSA): Is a mathematical cryptology technique used by digital currencies and Bitcoin to ensure the security of the peer-to-peer transactions using secret codes and keys.

Email Harvesting: The mechanism to obtain a large number of email addresses using different methods or techniques.

Email Spam: Unsolicited emails that are usually sent in bulk to nonspecific recipients.

Embodied Conversational Agent: Characters which are generated by informatic tools and they show properties which are specific of face to face human communication.

Emoji: A small digital image or icon used to express an idea, emotion, etc.

Empathy: The ability to understand or feel what another person is experiencing or feeling.

Encipherment: An algorithm used to convert a readable message into unreadable message. It is used in the field of security.

Encryption: The process of encoding a message or information in such a way that only authorized parties can access it using a decryption key.

Encryption-Decryption: An algorithm used to transform information to something random, meaningless and not readable, and then translate it back to something understandable.

Enron: A company in the United States which went bankrupt in 2001 due to accounting fraud. It has been dubbed the worst accounting scandal in history, and it was exposed through whistleblowing.

Entity Resolution: Entity resolution (ER) is the problem of algorithmically determining when two entities in a KG refer to the same underlying entity. For example, the same entity 'Barack Obama' may have been independently extracted from two webpages under names such as 'President Obama' and 'Obama'.

ETag: Entity Tag is a server-side identifier assigned to content for cache-control. The browser caches and sends the ETag on subsequent web requests, which allows the server to send the resource only if the server version has changed. ETag can also be used to track users uniquely, online.

Ethereum: Is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

Exploitation: Taking advantage of someone or something for personal gain.

Externalizing Difficulties: Includes children's and adolescents' failure to control their behaviors.

Fake News: Content that contains inaccurate, misleading, or fabricated information about current events, which is being distributed through different channels of communication such as print, broadcast, text messaging, or social media.

Fake Reviews: Product review produced with the goal of artificially improving (or damaging) the ratings of the product.

Fantasy-Driven Offender: Online sexual offenders who seek only online interactions with children; often marked by illicit messages, exhibitionism, and child pornography (Briggs et al., 2011).

Fear of Missing Out (FOMO): Some people are afraid to go offline in case they miss out on some exciting piece of news.

File-Sharing: Offering and transferring digital files via various channels of the internet, usually in a decentralized manner.

Filter: The implementation of KM strategy. A method used to separate the big data, data, information, or knowledge needed to make a specific decision from unneeded big data, data, information, or knowledge.

Firewall: A firewall is a network security system that allows or denies incoming and outgoing network traffic based on predetermined security rules.

Form Spam: It is a method of submitting web forms with unwanted information.

Fraud: A deceptive practice or series of acts that are designed to take advantage of individuals, systems, or other process for the benefit of someone else, usually for personal monetary gain.

Gateways to Cyber Abuse: Computer applications or apps, websites, social media networks, texting services and other communication modes which can digitally or electronically connect users to cyberspace (the internet).

GDPR: General Data Protection Regulation is a new set of rules governing the privacy and security of personal data laid down by the European Commission.

Generalized Method of Moments (GMM Estimation): It is a common method for estimation of the parameters in statistical models. Usually it is applied in the context of semiparametric models, where the parameter of interest is finite-dimensional, whereas the full shape of the data's distribution function may not be known, and therefore maximum likelihood estimation is not applicable. Using the moment conditions, the true parameter values are estimated. The GMM method then minimizes a certain norm of the sample averages of the moment conditions. It is applied in case when there can be a chance of endogeneity problem.

Ghostwriters: Individuals who conceal their true identities from detection by engaging in schemes intended to defraud.

Gini Coefficient: In economics, the Gini coefficient sometimes called Gini index, or Gini ratio, is a measure of statistical dispersion intended to represent the income or wealth distribution of a nation's residents, and is the most commonly used measurement of inequality.

Globalization: Increasing global awareness of economic, social and political interdependencies among states due to increasingly porous state barriers due to rapidly increasing commerce, finance, information and labor flows across these borders. Incentives to globalize ultimately relate to the imperative to develop a state's economic and political power resources through integration in the global capitalist production chain.

Global Platform: Is an organization that publishes the standard for secure mobile and embedded platform

Grey Zone Threats: These are the threats that comprise a full spectrum of means and tools used by aggressor states to subvert their rivals' plans and strategies. These kinds of threats are perceived as affordable, less risky and flexible by the aggressor states.

Grooming: Attempts by an adult to build a child's trust and interest before making sexual advances.

Hacker Culture: A subculture of individuals who abuse vulnerabilities in systems for a common goal.

Hacker Ethics: Principles and ideologies that are shared in hacker culture.

Hacking: Manipulation of a technological device to acquire data unlawfully within a system.

Hactivism: 1) The combination of 'hack' and 'activism' to explain the use of technology in the promotion of political or social change. 2) Political engagement around hacking activities and the access to free and independent information.

Hate Speech: Speech that attacks a group (or, sometimes, a person) based on categories like race, sex, religion, origin or disability. Its goal is to incite prejudice and spread bigoted views.

Health Research Fraud: Intentional misrepresentation of the methods, procedures, or results of healthcare research. Behavior characterized as scientific fraud includes fabrication, falsification, or plagiarism in proposing, performing, or reviewing scientific research, or in reporting research results. Health research fraud is unethical and often illegal. A good example of such fraud with major ramifications is the measles-autism link published in the lancet but retracted in 2010 when it was confirmed that the study was conducted dishonestly and irresponsibly, using bogus data. Nevertheless, this erroneous link is partly responsible for increasing refusals of Measles containing vaccines by parents.

Healthcare Fraud: An intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party. Healthcare fraud refers to illegal acts of misrepresentation and false claims in order to receive undue financial or healthcare advantages. Health care fraud accounts for between 2 and 10% of wasted health resources globally. The World Health Organization cites healthcare-related fraud as one of 10 leading causes of inefficiency in health systems. Web-based healthcare fraud is a major challenge, especially when signatories to health organizations' accounts siphon money into private bank accounts. Regular audits and electronic monitoring systems such as e-claims management services help to monitor and prevent healthcare fraud.

HFI: Human freedom index; a numerical measure of the personal and economic freedom available in a country. It is measured annually. The HFI is determined from an evaluation of over 70 different indicators for each measured country.

Homebrew: Software that the end-user codes and/or compiles for his own (and his friends) device. This software is not suctioned by the device manufacturer who receives no royalties.

HPKP: It is a safekeeping policy that tells a web client to associate a detailed cryptographic public key with a certain web server to cut the jeopardy of MITM attacks with bogus certificate.

HRM: Acronym for human resource management. A set of practices to attract, develop, and maintain an effective workforce.

HSTS: It is a web safekeeping policy contrivance that aids to protect websites against protocol downgrade outbreaks and cookie hijacking.

HTML5: Version 5 of hypertext mark-up language which was released in October 2014 added major improvements and features such as ability to handle multimedia and graphic features natively, and a web storage framework that can store data similar to previous usage of cookies.

HTTP: HyperText Transfer Protocol, the underlying protocol used by the world wide web. This protocol defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

HTTP Cookie: Due to security reasons, websites visited by an Internet user are not allowed to access the internal storage of the visitor's computer, such as the hard disk. The only way to store a small amount of data such as visitor's preferences, which is individual to each visitor is to store it within the browser's storage, as plain text. Such storage is called a cookie, which was in earlier browsers a text-based file on the visitor's computer. But now each browser decide how it stores. Though a browser may have many hundreds of cookies, each saved by a different website, each website can only access the cookie that it has placed, but not the cookies placed by another website.

Human Sex Trafficking: Inducing others to perform a commercial sex act by force, fraud, or coercion; as inducing a person under 18 years of age for such an act; and/or as recruiting, harboring, transporting, providing, obtaining a person for labor or services through the use of force, fraud, or coercion in order to subject them to involuntary servitude, peonage, debt bondage, or slavery (National Institute of Justice, 2012).

Human Trafficking: Modern day slavery or illegal transporting of people typically for the purposes of forced labor or sexual exploitation.

Hybrid Warfare: A recent term for reliance upon covert and informal policy tools for interference in the internal politics and policy making in target states. This term emerged concurrently with the development of the Internet as an infrastructure vehicle and as form of media communication. Covert and informal modes of international political competition and influence expansion acquired greater emphasis along with the post 1945 nuclear setting. The need to maximize the degree of control over potentially escalatory conflict dynamics pushed policy makers to obscure their international victories, defeats and stalemates in order to lessen the potential for provoking nationalist hostility that would lessen the political decisional latitude available to policy makers.

Hypercall: The term is analogous to System call. A call by a user process or the operating system for the hypervisor to perform some service required by the operating system of process.

Hypercomputation or Super-Turing Computation: Is a multi-disciplinary research area with relevance across a wide variety of fields, including computer science, philosophy, physics, electronics, biology, and artificial intelligence; models of computation that can provide outputs that are not Turing computable.

Hypervisor: A hypervisor is a type of computer software designed to run multiple operating systems on the same hardware.

Identification Warning Signs: Signs that showcase evidence of identifying with law enforcement, military paraphernalia, attackers, or assassin.

Identity Theft: The crime of stealing sensitive personal information, such as usernames, passwords, date of birth, social security number, and personal and financial information.

Illegal: Actions or practices which are against the law.

Indexing: The process followed by search engines to create an index of the contents present on the Internet, to allow easy retrieval when displaying results to user queries.

Individualism: The belief that each person is more important than the needs of the whole group or society.

Information and Communication Technology (ICT): Telecommunication technologies that provide access to information such as the internet, wireless networks, cell phones, and other communication mediums.

Information Extraction (IE): Information extraction (IE) is an algorithmic technique that generally accepts as input either text or raw HTML as input, and outputs a set of ontologically typed instances. For illicit domains, the investigative schema serves as the ontology. Supervised machine learning and deep learning IE methods have emerged as state-of-the-art in recent times.

Information Operations: Information operations are the part of political warfare/grey zone conflicts that occur in an asymmetrical way via social and conventional media, state organisations and military means to weaken the morale and psychology of enemy states.

Integrity: Being whole and having a consistent set of ethical, moral, and legal practices.

Internet: The Internet is an interactive medium based on a decentralized network of computers. The Internet may also be used to engage in other activities such as sending and receiving emails, money, trading files, exchanging instant messages, chatting online, streaming audio and video, every type of business purpose, and making voice calls.

Internet Blocking: Blocking access for users to certain Internet sites on a national level.

Internet Crime Complaint Center (IC3): It was established to provide people with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation (FBI) regarding cybercriminal activities and to develop cooperation with law enforcement agencies.

Internet of Things (IoT): IoT is a concept of connecting any device to the internet or other connected devices to send and receive data.

Internet Privacy: This is the privacy and level of personal data and or information published online (via the internet).

Internet Utilisation: The amount of data flowing through a computer or device (mobile phone, tablet) for a given period of time.

Intimate Partner: A close personal relationship between individuals who identify as a couple that is characterized by some of the following dimensions: emotional connection, regular contact, and ongoing physical contact that need not be sexual.

Intrusion: Wrongfully accessing a computer's system or network.

Intrusion Detection Systems: An intrusion detection system (IDS) is a hardware device or software application that monitors a network or systems for malicious activity or policy violations.

Investigative Schema: An investigative schema is an ontology expressing an investigative domain of interest, usually involving an illicit activity like sex advertising. The investigative schema is usually simple and shallow, hence the term 'schema' and not 'ontology'.

IP Address: Internet protocol address, the basic identifier of a computer participating in the internet. It can be seen as a pseudonym of the user of the computer and can be connected to the identity of the user by his internet service provider.

IRC: Internet relay chat (IRC) is a system for chatting that involves a set of rules and conventions and client/server software.

Isolation: LCT step used more by contact-driven offenders to separate victim from support network.

Key Exchange: A method of transferring a secret key among various users. This key may be needed in cryptography to protect many entities like information, system, etc.

Knowledge Graph (KG): A knowledge graph (KG) is a directed, labeled multi-relational graph that is used to model and represent semi-structured data to make it more amenable to machine reasoning ('knowledge').

L4: A family of microkernel operating systems by Liedtke initially. OKL4 and seL4 are operating systems that were derived from L4.

Law of Armed Conflict: The Law of Armed Conflict (LOAC), also known as the International Humanitarian Law, is a body of international law which regulates the behaviours of actors during armed conflict by ordering balance between military necessity and humanity. It comprises the Geneva Conventions, Hague Conventions and customary laws. It also limits the targeted attacks of combating parties in order to protect civilians and avoid total disaster.

Leakage Warning Signs: Signs that show-case evidence of communication to a third party of an intent to do harm to the target.

Legislation: Law enacted by a legislature.

Legislature: A body of individual persons empowered to legislate; specifically, an organized body authorized to make laws for a political entity such as a nation, state or province, or a city.

Link Spamming: The process of posting links on websites, discussion forums, blogs, and other web services that show user comments.

Local Area Network (LAN): Computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college.

LoM: Loss of money; personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

Loneliness: An unpleasant emotional response to isolation or lack of companionship.

Machine Learning: Is the use of artificial intelligence (AI) that provides systems with the capability to learn and automatically improve from experience (data) without being explicitly programmed.

Machine Learning Application: Is class of methods of artificial/natural intelligence, the characteristic feature of which is not a direct solution of the problem but training in the process of applying solutions to a set of similar problems.

Machine Learning Application With Avatar-Based Management Technique Use: Is a class of methods of natural intelligence, the characteristic feature of which is not a direct solution of the problem but training in the process of applying solutions to a set of similar problems.

Malicious Code: Computer code often used by hackers to infiltrate a computer to cause damage and security vulnerabilities.

Malspam: Spam emails that carry and deliver malware.

Malware: Malicious software that is designed to compromise a computer, server, or a computer network so as to gain unauthorized access or to cause damage.

Maoists: Maoists, also known as Naxalites or Naxals, are the group of people who believe in the political theory derived from the teachings of the Chinese political leader Mao Zedong. It is a doctrine to capture State power through a combination of armed insurgency, mass mobilization and strategic alliances. Also, these Maoists use insurgency doctrine based on use of propaganda and disinformation against State institutions. Herein, the author has used Maoists, left-wing extremists, and Naxalites interchangeably.

Masquerading: The creation of an anonymous or fake identity by an individual to harass another individual.

Maturity Models: Is a section of avatar-based management.

Metropolitan Area Network (MAN): A network that connects two or more local area networks together but does not extend beyond the boundaries of the immediate town, city, or metropolitan area.

Misinformation: False content that is the product of error (i.e., whose originator or distributor may not be aware that the content is not truthful).

Mobile Games: Digitally based games mostly played on mobile devices (e.g., smartphone, tablet) (DaCosta, Seok, & Kinsell, 2015).

Modchip: A hardware device that is soldered on top of existing product PCB replacing some chip. Usually, the modchip is designed to remove or disable the chip that handles copy protection.

Modus Operandi: The typical course of events in a criminal offence.

Money Laundering: The conversion of illegally obtained money to legitimate money and assets using legal businesses and transfer of currencies.

Monte Carlo Simulations: Monte Carlo simulation is a mathematical technique that generates random variables for modeling risk or uncertainty of a certain system. The random variables or inputs are modelled on the basis of probability distributions such as normal, log normal, etc. Different iterations or simulations are run for generating paths and the outcome is arrived at by using suitable numerical computations.

Mutual Legal Assistance (MLAT): MLAT are formal investigation request made by the states for the access of the data located in other country for the purpose of investigation and extradition.

Nation: A community which a nationalist believes should and can achieve national self-determination through acquiring a sovereign state for the nation if it does not already have such a state. If this community already has its own sovereign state, then the nationalist will be perceptually and emotionally preoccupied with challenges to this sovereign state, tending to equate the state, represented by its governmental apparatus, with the nation.

Nation State: A state in which the overwhelming majority of citizens show their primary self-identification with the territorial community within the state through favoring it more above any other identity group or community. Examples include the United States, Russia, China, Japan, Germany and others. Multinational states, such as the old Soviet Union and Yugoslavia as well as Iraq, are not nation states. Neither are multiethnic states nation states. Examples of the latter include most post-colonial African and many post-colonial Asian states including India. Non-nation states, and multinational states in particular, are subject to centrifugal political forces among ethnic groups seeking national secession and self-determination. These centrifugal forces may maintenance of liberal democratic political regimes highly problematic insofar as democratic elections produce ethnic nationalist leaders seeking self-determination. The communities of the old Yugoslavia as well as in the old Soviet Union continue to deal with such secessionist and irredentist nationalist forces.

Nationalism: A form of intense ingroup political loyalty opposing perceived challenges to the sovereignty of the nation. It is characterized by relatively intense emotional affect and perceptual stereotyping of self and other, outgroups stereotypically perceived as challenges to the nation. A community behaves nationalistically when the modal, politically attentive citizen is a nationalist.

Nationalist: An individual who sees himself/herself as a member of a large group of people who constitute a community that is entitled to independent statehood and who is willing to grant that community a primary and the primary terminal loyalty.

Netrespass: Infiltrating another internet user's space and carrying out unauthorised activities (e.g., trespass).

News Scraping: It is a process of scraping the news from the newspaper websites.

Nonconsensual Pornography: The distribution of sexually graphic images, including through digital platforms, of individuals without their consent. This is also referred to as “revenge porn,” “cyber rape,” and “involuntary porn.”

Normal World (Insecure World): The normal operating system that the given platform is running for normal applications. In most cases, this refers to Google’s Android or Apple’s IOS.

Normative Belief: Beliefs about the acceptability and tolerability of a behavior.

Object-Oriented Ontology: Object-oriented ontology (OOO) is a school of thought which argues that objects exist independently of human understanding and perception. The term was coined by the philosopher Graham Harman. It is also designated in the existing literature as ‘speculative realism’, which criticises the reductionism of Kantian philosophy.

Onion: A hidden Internet domain that disguises a site’s true Internet (IP) address. Onion domains are accessed using TOR, usually through a specially designed Internet browser.

Online Child Sexual Exploitation: Use of information technology including social media, webcams, or cell phones to solicit or coerce children to engage in illegal or inappropriate sexual activity.

Online Communication: Any kind of communication between either individuals or organisations that occurs on the internet.

Online Phishing: An online criminal attempt via fraudulent emails, web links, and websites to trick online users to surrender sensitive private information.

Ontological Approach to Cyberspace: It basically assesses cyberspace as a metaphysical laboratory that combines art and philosophy of things, machines and different domains, although this philosophical approach is not new.

Ontology: An ontology may be practically defined as a controlled set of terms and constraints for expressing the domain of interest. An ontology can range from a simple set of terms (e.g., {PERSON, LOCATION, ORGANIZATION}) to a taxonomy (with concepts and sub-concepts e.g., ACTOR and ENTREPRENEUR would be sub-concepts of PERSON) to a general graph with equational constraints e.g., that the domain and range of the relation starred-in is ACTOR and MOVIE respectively. Any KG that is ontologized thus should obey such constraints at the instance level.

Open Coding: The process of repeating readings of media sources and a line-by-line analysis of the data in order to open up the data to understand the meanings and concepts in it. Open coding includes the labelling of concepts and creating categories for comparison.

Optimism Bias: A human tendency where people overestimate the likelihood of good things and underestimate the likelihood of bad things happening onto them.

Panel Data: Also called longitudinal data, represents cross-sectional time series data i.e. data on multi-dimensional cross-sections (comprising of individuals, firms and countries) over a period of time.

Paper Mills: Business entities created for the sole purpose for selling scholarly works and publications written by ghostwriters.

Parental Mediation and Monitoring: The strategies that parents use to manage the relationship between their children and media.

Parenting Style: The standard strategies that parents use in their child rearing.

Patient Safety: Initiatives to assure freedom from accidental or preventable injuries produced by medical care. Emphasis is placed on the system of care delivery that prevents errors, learns from the errors that do occur, and is built on a culture of safety that involves health care professionals, organizations, and patients. With the expansion of internet technology in the use of medical devices such as cardiac pacemakers, patient safety is increasingly vulnerable to web-based attacks, which have serious repercussions.

Payment Gateway: An online service that facilitates cashless transactions.

Peer Attachment: The internalization of the knowledge that their peers will be available and responsive.

Peer Contagion: The transmission or transfer of deviant behavior from one adolescent to another.

Peer Support: A situational process in which respect and support principles characterize the relationships involving people with common experiences.

Peer-to-Peer: A distributed service whereby one person communicates with another, without intermediation by an outsider.

Peer-to-Peer Network: A network of nodes with usually equal rights and responsibilities. The nodes are usually computers of Internet users where a software with the peer-to-peer protocol is running.

Periodicity: Periodicity is the occurrence of similarity in more or less regular intervals and is a property exhibited by many processes that are of interest in a variety of scientific disciplines.

Personal Area Network (PAN): A network typically involving small devices organized around an individual person.

Perverved Justice: A grass-roots vigilante organization where volunteers pose as children online in order to expose offenders.

Phishing: A method of cyberattack which is employed to capture sensitive information including passwords and personal information for malicious purposes through means such as deceptive emails.

Plagiarism: Individuals who intentionally create and publish false information to gain an advantage or benefit.

Polarization: Intra-societal stereotyping due to intensifying perceived challenges from other constituencies within a polity, with the different contestants portraying the other as disloyal, even treasonous, to the nation and its state. Polarization is most likely to intensify when certain constituencies within the polity portray their favored policy prescriptions for the perceived well-being of the nation as religiously, i.e. divinely mandated. Secular opponents, therefore, are more likely to be stereotyped as evil and disloyal.

Police Force: A body of trained officers entrusted by a government with maintenance of public peace, law and order, enforcement of laws, and prevention and detection of crime.

Poverty Head Count Ratio: The poverty head count ratio (PHCR) is the proportion of a population that exists, or lives, below the poverty line.

Power: The exercise of influence over the minds and actions of others.

Predictive Analytics: Is the use of data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on empirical data.

Price Scraping: It is a process of extracting or collecting the prices of various items in e-commerce site available over the internet without the consent.

Prior Ethos: Image of the self before the discussion (perception of the self by others).

Privacy: Ensuring privacy involves citizens having control over existing information about themselves and exercising this control in a consistent manner with their personal interests and values.

Privacy Paradox: Individuals often claim to be concerned about threats to their privacy, yet do not act to protect their personal information.

Privacy Protection: The coexistence of the collection and dissemination of information communication technologies, what the public expects as well as socio-political and legal concerns bounding them.

Private Browsing Mode: A privacy feature in web browsers that disables a user's browser and search history.

Private Cyberstalker: A perpetrator of cyberstalking for personal motives.

Private Health Data: Is defined as individually-identifiable health data, which is exquisitely sensitive. Being linked to an individual, the private health data can only be shared with the permission of the individual.

Privilege Ring: Intel architecture defines several privilege “rings” (protection rings) that refer to the current state of the system. These rings are ring 3 (user mode) where certain operations as not allowed, ring 0 (supervisor mode/operating system mode) where access to hardware devices is allowed, and hypervisor mode (ring –1) where hypervisor operations are allowed. Rings 1 and 2 also exist: these “in-between” privilege levels had historical usage but are mainly unused in modern systems.

Proof-of-Work: An algorithm used to affirm transactions and produce new blocks to the chain.

Protection Motivation Theory: This concept attempts to explain the way in which individuals react to perceived threats, and holds that individuals consider the perceived severity and probability of a threat, as well as the efficacy of their potential response.

Provictim Attitudes: The belief that bullying is unacceptable and that defending victims is valuable.

Pseudo-Child: A law enforcement officer or a volunteer posing as a child in a chatroom.

Public Sphere: The area of political and cultural discourse of the modern actor.

Query Reformulation: Query reformulation refers to a set of techniques wherein a query (in some domain-specific language like SPARQL or SQL) that is originally posed against a DSS engine is reformulated into a set of queries (in the same or different language) to increase query retrieval performance. Query reformulation is a useful technique both when the underlying KG is noisy and when the original query does not fully express (or over-conditions) user intent.

Raising Concerns Policy: Otherwise labelled “freedom to speak up” and “internal whistleblowing” such policies provide standardization of internal channels for speaking up about illegal or unethical practices and provide support and required anonymity for the employee who raises a concern.

Random Forest Classifier: Random forest classifier uses a set of decision trees from randomly selected subset of the training data and then aggregates the decision from each set to arrive at the final decision class of the test data. This improves accuracy and avoids over-fitting and hence better than decision tree algorithms.

Ransomware: Is defined as the illegal access to computer system using malware for the purpose of gaining control of the system with the motivation for financial gains.

Red Pill: Red pill is a type of software that is used to detect and defeat blue pills. The goal of the red pill is to provide an answer to the question, “Is the computer currently running a blue pill?” in the most reliable possible method.

Relational Ethics: A contemporary approach to ethics that situates ethical action explicitly in relationship. An important context of such relationships is within organizations, in which employees and employers have roles and responsibilities. Organizational policies and codes of conduct (and in some nations, anti-defamation laws) usually explicitly prohibit employees from discussing or exposing company secrets to the media or third parties without management approval. Thus, external whistleblowers are implicitly violating the relational ethics of such organizations.

Revenge Porn: Sexually explicit images sent or posted without a person’s consent; often used to intimidate or embarrass.

Rich Execution Environment (REE): Rich Execution Environment is another area inside the main processor. The Rich Execution Environment runs a separate operating system. Usually, Google’s Android or Apple’s iOS. The Rich Execution Environment refers to the standard operating system that the device is running. The Rich Execution Environment offers significantly more features and applications and as a result, is vulnerable to attacks.

Risky Online Behavior: A risky online behavior is an action that can potentially leave one exposed to a variety of dangers, putting individual and possibly organizational internet security at risk.

Romance Scams: Social media are used to establish a relationship of trust between the perpetrator and the victim. As soon as the victim transmits confidential pictures or videos to the perpetrator, the perpetrator abuses them for blackmail purposes.

Rootkit: Rootkit is malicious software that grants unauthorized user-persistent access to the victim computer resources. The rootkit is also designed to mask its existence such that the administrator will not be able to detect it.

Router: Router is an inter-networking device that forwards the packets from one computer network to another. Routers perform the traffic route finding on the Internet by means of a routing table.

RtoEx: Reluctance to express; the reluctance to freely express oneself online or on the internet.

RtoExC: Reluctance to express due to concerns of possible consequences or safety; the reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.

RtoExnonC: Reluctance to express when users are not reminded of possible consequences or safety issues resulting from the expression.

Scam: A dishonest scheme used to deceive and manipulate a person into voluntarily providing valuable assets or information.

Scenography: Study of the scene frame (concrete location, definition of the setting).

Secure Communication: A method of transferring information on the internet securely.

Secure World: Secure world is the name for the secure, trusted execution environment (TEE) on ARM Architecture. It is running concurrently, on the same CPU as the normal world. However, ARM provides hardware and software mechanisms to ensure that the normal world and secure worlds are running on separate environments.

Security: A set of measures taken to protect oneself from any acts of violence, such as attacks, robberies, espionage, sabotage, etc.

Select Committee on Deliberate Online Falsehoods: In 2018, a Select Committee on Deliberate Online Falsehoods was set up by Singapore's parliament to examine and report on the phenomenon of the use of digital technology to spread falsehoods online. They have since unveiled 22 recommendations to combat online falsehoods.

Selective Coding: The process of further linking the categories from axial coding into a core category. This process takes place after axial coding.

Session Hijacking: Using a spoofed IP address or Man-in-the-Middle techniques to impersonate a legitimate host to eavesdrop or redirect network communication.

Sexting: A common practice among young persons, which involves taking sexually explicit images of one's self and sending it to others via ICTs.

Sextortion: A form of sexual exploitation during which the victim is coerced to provide sexual favors (including child pornography material) to the perpetrator.

Sexual Exploitation: Taking advantage of a person sexually for personal gain or make profit.

Shareable Content Object Reference Model (SCORM): Is a collection of standards and specifications for web-based electronic educational technology (also called e-learning).

SIEM: Security information and event management.

Signature-Based Classifier: Signature-based classifier classifies items based on an entry in a lookup table with signatures and the corresponding class labels. Hence, this classifier is not efficient in detecting novel patterns/signatures.

Singular Value Decomposition (SVD): A factorization mathematical algorithm of matrices used in diverse application such as signal processing, communication, and imagery.

Sleptsov Net (SN): Is a bipartite directed multi-graph supplied with a dynamic process.

Smart Contract: Is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other.

Smuggling of Migrants: The facilitating of illegal entry of a person into a country he or she is not a national or resident of.

Social: Engineer: A person who is expert on the social engineering techniques, he uses deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Social Aberration: Diversion from common social values and norms.

Social Comparisons: As a result of using social networking sites some people may get the impression that other users are leading better lives in comparison to their own.

Social Engineering: The psychological manipulation of victims by cyber perpetrators, in order to get victims to divulge sensitive confidential information, or to perform certain actions that help perpetrators to successfully execute their cyberattacks.

Social Engineering Attack: Various manipulation techniques to elicit sensitive information, manipulating a person into giving information to the social engineer.

Social Exchange Theory: A behavioral theory that seeks to explain the interaction between a person and another person or entity. Its fundamental proposition is that the interaction is influenced by the person's evaluation of the interaction's risks versus rewards.

Social Exclusion: The process involving individuals or groups of people block or deny someone from the group.

Social Network: A social network is an online communication platform that is used for creating relationships with other people who share an interest, background or real relationship.

Social Network Security: The process of analyzing dynamic social network data in order to protect against security and business threats.

Social Networking Sites: Social networking sites (SNS) enable users to interact with other people online; similar to how people may socially interact offline by sharing personal experiences, images, making plans, and so forth.

Sociology of Crime: A science discipline that examines the phenomenon of crime through a sociological approach in its historical process.

Spam: Messages sent via the internet often unimportant with the intent to advertise, induce malware and phishing programs.

Spamming: It is an exploitation of messaging systems to broadcast unwanted messages.

Spear Phishing: Phishing for sensitive information by using personalized emails containing malicious attachments or fraudulent web links to target specific members or groups of an organization.

SSL: It is the foundation of the Internet protection. It secures website and handles the confidential and sensitive information of the users like credentials by providing critical security, privacy and data integrity.

Stalking: A person's location may be tracked without their knowledge or permission through the use of technology, by someone who is interested in their whereabouts or someone who holds a grudge; therefore, it is an invasion of personal privacy, ethically unacceptable, and potentially a safety threat.

Stateful Tracking: Using identifiable information stored in a user's local computer, such as an HTTP cookie to identify a visitor's computer uniquely on the internet.

Stateless Tracking: Does not store any identifiable information on a user's computer. A combination of unique signatures about each computer is stored in the tracking server, which can identify a computer with a relative high accuracy, but not as precisely as stateful tracking methods.

Steganography: A technique that aims to hide information or files inside an electronic file so that no one suspects such files or information is being delivered.

Stereotype: A simplified perception of the political environment, specifically regarding policy targets. Differences in stereotypical patterns in perception emerge along with different types of perceived challenges to the perceiver from a target. An intensely threatening target of perceived equal capability and techno-cultural level will tend to be perceived as a diabolical enemy. A perceived weak, inconsistent and unmanageable target unable to resist the perceiver's greater will and determination to achieve its objectives will tend to be perceived as degenerate. Dangerous adversaries perceived as superior in capability and techno-cultural capabilities will tend to be perceived as an imperial threat. Perceived weaker targets in capability and culture ripe for exploitation to achieve some other overarching objective, i.e. containment of a great power enemy, will be perceived as a colonial target of opportunity. Troublesome, threatening weaker targets in culture and capability will tend to be perceived as criminal rogues.

Surface Web: It can be defined as that portion of the internet whose websites are indexed by search engines such as Google, Yahoo, and others. They are easily accessible and do not require the use of special software as needed for the deep web.

TChS: Thinking about and changing settings; time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.

Technical Subterfuge: The act of deceiving victims and stealing their sensitive information by technical means.

Thin Hypervisor: A hypervisor that is designed to support only one operating system.

Third-Party Applications: An application that is provided by a vendor other than the manufacturer.

Threat: The possibility of malicious attempt to damage or disrupt a computer or system.

Threat Assessment: Threat assessment is a structured group process used to evaluate the risk posed by a student or another person, typically as a response to an actual or perceived threat or concerning behaviour.

TLS: The upgraded version of SSLv3.

TMT: Too much time; the belief that cybersecurity risk amelioration requires excessive usage of one's time.

TOR: The Onion Router is a free downloadable software that hides the IP addresses of computers via using multiple encrypted relays. Thus protecting user identity from traffic analysis.

Traditional Bullying: An escalating process in which one or more employees are subjected to negative psychological and physical abuse recurring over an extended period of time, where the target is reduced to a psychologically inferior state and it creates a hostile work environment to those exposed.

Traditional Face-to-Face Bullying: The use of strength or influence to intimidate or physically harm someone.

Trafficking in Persons: Human trafficking or the recruitment, transfer, transportation, or harboring of people by coercion or force, abduction, fraud, deception.

Transhumanism: Ideology that promotes the development of human beings through their interaction with artificial intelligence.

Trusted Computing (Trusted Systems): Trusted systems are systems that are supposed to behave in a certain predefined way (for example, verify DRM). Local and remote software can attest that the system is indeed a trusted system before executing code.

Trusted Execution Environment (TEE): A Trusted Execution Environment (TEE) is a secure area inside the main processor. The trusted execution environment runs a separate operating system in parallel to the main operating system in an isolated environment. The trusted execution environment guarantees the confidentiality and integrity of the code and data loaded in the TEE.

Trusted Platform Module (TPM): The Trusted Platform Module (ISO/IEC 11889) is an international standard and specification for a secure cryptoprocessor. The TPM is a dedicated microcontroller designed with hardware obfuscation to prevent tampering. The TPM provides cryptographic operations and can measure the CPU and running software for platform attestation.

TrustZone™: An ARM Exception level that allows running TEE in a secure environment in parallel to the normal ARM environment.

UN: United Nations.

Unethical: Actions or practices deemed immoral or wrong.

USA Patriot Act: The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 which granted the federal government increased control in monitoring and interrupting networks in order to counterbalance terrorist attacks.

User Account: An established technique for connecting a user and an information service.

Veracity: Conformity to facts; accuracy. Veracity is often difficult to establish in whistleblowing contexts since most whistleblowers have only limited information on a specified issue. Consequently, a significant proportion of external whistleblowing incidents have been found to be false. Contemporary whistleblowing laws such as the 2019 law in Australia require whistleblowers to provide objective evidence as condition to raising concerns internally or externally.

Victim: The individual or entity that suffers the effect of cyberattacks.

Video Games: Digitally based games typically played on personal computers or dedicated gaming devices, such as game consoles (e.g., Xbox, PlayStation) or handheld game devices (e.g., 3DS, Vita) (DaCosta et al., 2015).

Violent Extremism: A willingness to use or support the use of violence to further particular beliefs, including those of a political, social, or ideological nature. This may include acts of terrorism.

Virtual Child Pornography: Child pornography produced by digitally modifying pre-existing images or fully generated by a computer.

Virtual Circuit: Virtual circuit is a path for the flow of data packets over a network, which does not exist in reality. It is ‘virtual’ in the sense that there is no dedicated physical layer link between the source and the destination of the data.

Virtual Private Network (VPN): A virtual private network (VPN) provides a means of connecting to a network within an organisation (as if you were inside the organisation) even though you are not physically present.

Virtual Reality: A virtual environment that simulates reality in which human being can be immersed through tools like glasses and visors. Depending upon different tools, the user can receive and respond to different stimuli.

Virtue Ethics: Person rather than action based ethical conduct. It analysis at the virtue or moral character of the person carrying out an action, rather than at ethical duties and rules, or the consequences of particular actions. When morally orthodox and benevolent, virtue ethics is closely aligned to the ethical principle of deontology – fulfilling a virtuous moral duty. Many whistleblowers claim that their decision to expose alleged wrongdoing in their organizations were motivated by the desire to act according to their moral character to prevent harm to innocent others.

Vulnerability: It is defined as a defect, imperfection, weakness, or inadequacy of a system.

Warez: Term for illegal digital goods, usually software or multimedia files.

Warning Signs: Warning signs are acts which constitute evidence of increasing or accelerating risk.

Web Scraping: The process of extracting data from the websites in a systematic manner.

Web Spoofing: Using fake websites to phish and trick users into giving up their personal information.

Whaling: A special type of spear phishing that targets high-rank individuals such as executives of an organization.

Whistleblower: An individual who reveals wrongdoing to some higher authority. Illegal and unethical activities are usually revealed by such a person.

Whistleblowing: Non-obligatory act of disclosing information about unethical or criminal activity in an organization. Internal (intra-organizational) whistleblowing is less damaging to organizational credibility and the careers of whistleblower than external whistleblowing – reporting to the media or anti-corruption or institutional ethics boards. The term whistleblower comes from the whistle a referee uses to indicate an illegal or foul play. Ralph Nader coined the phrase in the early 1970s to reduce stigmatization of individuals who report illegal activity, any of whom were at the time referred to as “rats” and “snitches”. There are no public cases of cybersecurity whistleblowers on record to date, but in countries like the United States where large organizations have minimum mandatory cybersecurity requirements and payments of up to 30% may be received for whistleblowing acts which lead to recovery of assets from the Securities and Exchange Commission, a strong potential exists for such cases to emerge.

Wide Area Network (WAN): A group of computer networks connected together over a large geographical distance crossing metropolitan, regional, or national boundaries.

Wi-Fi: Wireless Fidelity, a standard technology for wireless access to local networks. This technology allows electronic devices to be connected to a wireless local area network (WLAN) and Internet using radio waves.

Winmax: Technology that allows the expansion of the internet signal at higher speeds over long distances.

Workplace Cyberbullying: An escalating process in which an employee is subjected to perceived psychological abuse recurring over a period of time where the perpetrator uses some form of technology.

World Wide Web: The world wide web (WWW) is a network of online content on the Internet that allows documents to be connected to other documents by a link and enable the user to search for information by browsing on the net.

Zigbee: Protocol that is employed for PANs and is based on the IEEE 802.15 standard. Even though they are low-powered, Zigbee devices can transmit data over long distances by passing data through intermediate devices to reach more distant ones, creating a mesh network.

Compilation of References

- Aakhus, M. (2017). The Communicative Work of Organizations in Shaping Argumentative Realities. *Philosophy & Technology*, 30(2), 191-208. doi:10.1007/13347-016-0224-4
- Abadzi, H. (2006). *Efficient learning for the poor: Insights from the frontier of cognitive neuroscience*. Washington, DC: IBRD/World Bank. doi:10.1596/978-0-8213-6688-2
- Abburu, S., & Babu, G. S. (2013). A frame work for web information extraction and analysis. *International Journal of Computers and Technology*, 7(2), 574–579. doi:10.24297/ijct.v7i2.3459
- Abdul Rahman, M. F. (2019). Leveraging smart technology for better counter-terrorism intelligence. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 73–97). Singapore: World Scientific Press.
- Abel, R. (2016, September). Study finds gamer cyber hygiene stinks. *SC Media US*. Retrieved from <https://www.scmagazine.com/study-gamers-actively-shut-off-security-software-if-it-inhibits-game-play/article/530161/>
- Abel, R. (2018, June 18). Despite advancements, employees still practice bad cyber-hygiene, study. *SC Media*. Retrieved from <https://www.scmagazineuk.com/despite-advancements-employees-practice-bad-cyber-hygiene-study/article/1486713>
- Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Schneier, B. (1997). *The risks of key recovery, key escrow & trusted third party encryption; A report by an ad hoc group of cryptographers and computer scientists*. Retrieved from <https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W>
- Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*. doi:10.1093/cybsec/tyv009
- Abera, T., Asokan, N., Davi, L., Ekberg, J. E., Nyman, T., Paverd, A., ... Tsudik, G. (2016, October). C-FLAT: control-flow attestation for embedded systems software. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 743-754). ACM. 10.1145/2976749.2978358
- Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data*. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf
- About The Open Web Application Security Project - OWASP. (2018). Retrieved December 7, 2018, from https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project
- Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal*, 15(1), 5-31. doi:10.11610/Connections.15.1.01

- Acar, K. V. (2017). Webcam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology*, 11(1), 98–109.
- Accenture and Ponemon Insitute. (2017). *2017 cost of cyber crime study: Insights on the security investments that make a difference*. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
- Accenture. (2017). *Cost of Cybercrime Study*. Ponemon Institute. Retrieved November 2, 2018, from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
- Access to Information and Privacy Act (Zimbabwe). (2002).
- Ackerman, R. K. (2019, April 1). NATO Cyber Policy under Construction. *Signal*. Retrieved from <https://www.afcea.org/content/nato-cyber-policy-under-construction>
- Ackland, R. (2013). *Web social science: Concepts, data and tools for social scientists in the digital age*. London: Sage Publications.
- Adaja, T., & Ayodele, A. (2013). Nigerian youths and social media: Harnessing the potentials for academic excellence. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 2(5), 65–75. doi:10.12816/0001189
- Adams, W., & Flynn, A. (2017). *Federal Prosecution of Commercial Sexual Exploitation of Children Cases, 2004-2013* (No. NCJ 250746). Bureau of Justice Statistics. Retrieved from <https://www.bjs.gov/content/pub/pdf/fpcsecc0413.pdf>
- Adamson, F.B. (2005). Globalisation, Transnational Political Mobilisation, and Networks of Violence. *Cambridge Review of International Affairs*, 18(1), 31-49. doi:10.1080/09557570500059548
- Adams, W. R. (2017). High-accuracy detection of early Parkinson's Disease using multiple characteristics of finger movement while typing. *PLoS One*, 12(11), e0188226. doi:10.1371/journal.pone.0188226 PMID:29190695
- Africa.aspx. (2006). Zimbabwe: Econet and Telecel seek court order to block new regulation. *The Herald*. Retrieved December 11, 2018, from <http://www1.herald.co.zw/inside.aspx?sectid=11033&cat=1&livedate11/6/2006>
- African Charter on Human and Peoples' Rights, adopted June 27, 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 ILM 58, art. 9 (entered into force Oct. 21, 1986).
- African Union. (2014). *African Union Convention on Cybersecurity and Personal Data Protection*. Author.
- Agatston, P., Kowalski, R., & Limber, S. (2012). Youth views on cyberbullying. In J. W. Patchin & S. Hinduja (Eds.), *Cyberbullying Prevention and Response: Expert Perspectives* (pp. 55–71). New York, NY: Routledge.
- Aggarwal, C. C., Al-Garawi, F., & Yu, P. S. (2001, April). Intelligent crawling on the World Wide Web with arbitrary predicates. In *Proceedings of the 10th international conference on World Wide Web* (pp. 96-105). ACM. 10.1145/371920.371955
- Agrawal, S., & Agrawal, K. (2013). Deep Web Crawler: A Review. *International Journal of Innovative Research in Computer Science & Technology*, 1(1), 12–15.
- Ahmed, F., & Abulaish, M. (2012, June). An mcl-based approach for spam profile detection in online social networks. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 602-608). IEEE. 10.1109/TrustCom.2012.83
- Ahmed, E., Yaqoob, I., Hashem, I., Khan, I., Ahmed, A., Imran, M., & Vasilakos, A. (2017). The role of big data analytics in Internet of Things. *Computer Networks*, 129, 459–471. doi:10.1016/j.comnet.2017.06.013

Compilation of References

- Ahmed, S., Kabir, A., Sneha, S. S. A., & Jafrin, S. (2017). Cyber-crimes against womenfolk on social networks: Bangladesh context. *International Journal of Computers and Applications*, 174(4), 9–15. doi:10.5120/ijca2017915407
- Aiken, M., Moran, M., & Berry, M. J. (2011). *Child abuse material and the Internet: Cyberpsychology of online child related sex offending*. Paper presented at the 29th Meeting of the INTERPOL Specialist Group on Crimes against Children, Lyons, France.
- Aiken, M., Mahon, C. M., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). *A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online*. Taylor & Francis.
- Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70–89.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-T
- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.
- Akatyev, N., & James, J. I. (2015). *Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. Revised Selected Papers*. Springer International Publishing.
- Akdeniz, Y. (2008). *Internet Child Pornography and the Law National and International Responses*. Ashgate.
- Aked, S. (2011). An investigation into darknets and the content available via anonymous peer-to-peer file sharing. In *9th Australian information security management conference* (p. 10). Academic Press.
- Akter, F. (2018, June 17). *Cyber violence against women: The case of Bangladesh*. Retrieved from <https://www.genderit.org/articles/cyber-violence-against-women-case-bangladesh>
- Al Nashmi, E., North, M., Bloom, T., & Cleary, J. (2017). Promoting a global brand: A study of international news organizations' YouTube channels. *The Journal of International Communication*, 23(2), 165–185. doi:10.1080/13216597.2017.1300180
- Alanezi, F., & Brooks, L. (2014). *Combatting online fraud in Saudi Arabia using general deterrence theory*. GDT.
- Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *Management Information Systems Quarterly*, 25(1), 107–136. doi:10.2307/3250961
- Albanses, J. S. (2011). *Albanese Jay S, Transnational Crime and the 21st Century Criminal Enterprise, Corruption, and Opportunity*. Oxford University Press.
- Al-Daraiseh, A. Al-Joudi, A., Al-Gahtani, H., & Al-Qahtani, M. (2014). Social Network's Benefits, privacy, and Identity Theft: KSA case study. *International Journal of Advanced Computer science Application*, 5(12), 129-143.
- Aldea, A., Banares-Alcantara, R., Bocio, J., Gramajo, J., Isern, D., Kokossis, A., . . . Riano, D. (2003). An ontology-based knowledge management platform. In *Proceedings of the Workshop on Information Integration on the Web* (pp. 7-12). Academic Press.
- Alderman, K. (2012). Honor Amongst Thieves: Crime and the Illicit Antiquities Trade. *Honor Amongst Thieves: Crime and the Illicit Antiquities Trade*, 45(3), 602-627. Retrieved October 30, 2018, from <http://journals.iupui.edu/index.php/inlawrev/article/view/18002/18120>

- Aldoriso, J. (2018, March 26). What is cyber hygiene? A definition of cyber hygiene, benefits, best practices, and more. *Digital Guardian*. Retrieved from <https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>
- Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*. SSRN Electronic Journal.
- Aldridge, J., & Décary-Hétu, D. (2016). Cryptomarkets and the future of illicit drug markets. *Insights*, 21, 23–29.
- Alexa. (2016, July). *The top 500 sites on the web*. Retrieved from <http://www.alexa.com/topsites/countries;1/DE>
- Alexa. (2018). *The top 500 sites on the web*. Retrieved Oct 2, 2018 from <https://www.alexa.com/topsites>
- Alexander, M. (2016). Methods for Understanding and Reducing Social Engineering Attacks. Retrieved from <https://www.sans.org/reading-room/whitepapers/critical/paper/36972>
- alexbafana. (2016). *Smart-Contract Languages Comparison*. Retrieved from <https://steemit.com/smart/@alexbafana/smart-contract-languages-comparison>
- Alfie, A. (2016). Campañas Personalizadas. *Clarín*. Available at https://www.clarin.com/politica/usaran-confidenciales-anses-publicidad-oficial_0_HyY9MSEO.html
- Al-Furiah & Al-Braheem. (2009). Comprehensive study on methods of fraud prevention in credit card e-payment system. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services (iiWAS '09)*. ACM.
- Algarni, A., & Xu, Y. (2013). Social engineering in social networking sites: Phase-Based and Source-Based models. *International Journal of e-Education, e-Business, e- Management Learning*, 3(6), 456–462.
- Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, 26(6), 661–687. doi:10.105741303-017-0057-y
- Algerian National Extradited from Thailand to Face Federal Cyber Crime Charges in Atlanta for SpyEye Virus. (2013). Retrieved from The FBI, Federal Bureau of Investigation: <https://archives.fbi.gov/archives/atlanta/press-releases/2013/algerian-national-extradited-from-thailand-to-face-federal-cyber-crime-charges-in-atlanta-for-spyeye-virus>
- AlHogail, A. (2018). Improving IoT Technology Adoption through Improving Consumer Trust. *Technologies*, 6(3), 1–7. doi:10.3390/technologies6030064
- Ali, A., Khan, M., Saddique, M., Pirzada, U., Zohaib, M., Ahmad, I., & Debnath, N. (2016). TOR vs I2P: A comparative study. In *2016 IEEE International Conference on Industrial Technology (ICIT)* (pp. 1748–1751). IEEE. 10.1109/ICIT.2016.7475027
- Alim, S. (2016). Cyberbullying in the World of Teenagers and Social Media: A Literature Review. *International Journal of Cyber Behavior, Psychology and Learning*, 6(2), 68–95. doi:10.4018/IJCBPL.2016040105
- Ali, S. T., Sivaraman, V., Radford, A., & Jha, S. (2015). A survey of securing networks using software defined networking. *IEEE Transactions on Reliability*, 64(3), 1086–1097. doi:10.1109/TR.2015.2421391
- Alkiviadou N. (2017), Regulating Internet Hate: A Flying Pig? *JIPITEC*.
- All about digital banking fraud prevention. (n.d.). Retrieved from Net Gaurdians: <https://www.netguardians.ch/digital-banking-fraud/>

Compilation of References

Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2019). The Welfare Effects of Social Media. *National Bureau of Economic Research*. Working Paper 25514. Retrieved from <https://www.nber.org/papers/w25514.pdf>

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *The Journal of Economic Perspectives*, 31(2), 211–236. doi:10.1257/jep.31.2.211

Allcott, H., Gentzkow, M., & Yu, C. (2019). *Trends in the diffusion of misinformation on social media*. Research & Politics. doi:10.3386/w25500

Allen, T. S., & Moore, A. J. (2018). Victory without Casualties: Russia's Information Operations. *Parameters*, 48(1), 59-71. Retrieved from https://ssi.armywarcollege.edu/pubs/Parameters/issues/Spring_2018/9_Allen_VictoryWithout-Casualties.pdf

Allow States and Victims to Fight Online Sex-Trafficking Act of 2017 (2018), Pub. L. No. 115-164, 132 Stat. 1253.

Allyn, B. (2018, May 25). Digital ambulance chasers? Law firms send ads to patients' phones inside ERs. *NPR*. Retrieved from <https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers>

Almeida, F., Oliveira, J., & Cruz, J. (2010). Open Standards and Open Source: Enabling Interoperability. *International Journal of Software Engineering and Its Applications*, 2(1), 1–11. doi:10.5121/ijsea.2011.2101

Almeida, M. B., & Barbosa, R. R. (2009). Ontologies in knowledge management support: A case study. *Journal of the American Society for Information Science and Technology*, 60(10), 2032–2047. doi:10.1002/asi.21120

Alm, S. (2001). *The Resurgence of mass unemployment. Studies of the social consequences of joblessness in Sweden in the 1990s*. Stockholm: Swedish Institute for Social Research.

Alqubaiti, Z., Li, L., & He, J. (2016). The Paradox of Social Media Security: Users' Perceptions versus Behaviors. In *Proceedings of the 5th Annual Conference on Research in Information Technology - RIIT '16* (pp. 29–34). Boston: ACM Press. doi:10.1145/2978178.2978187

Alrwais, S., Yuan, K., Alowaisheq, E., Li, Z., & Wang, X. (2014). Understanding the dark side of domain parking. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)* (pp. 207-222). Academic Press.

Al-Shibli, M. (2015, Oct.). Dynamic UAS Image Encryption-Decryption Using Singular Value Decomposition (SVD) and Random-Poisson-XOR-Keys Techniques. *International Journal of Unmanned Systems Engineering*.

Al-Shibli, M., Marques, P., & Spiridon, E. (2018). Artificial Intelligent Drone-Based Encrypted Machine Learning of Image Extraction Using Pretrained Convolutional Neural Network (CNN), Big Data and Machine Learning (BDML) 2018. ACM.

Al-Shibli, M. (2015). UAS Image Encryption-Decryption Using Singular Value Decomposition (SVD) and Random-Poisson-XOR-Keys Techniques. *World Congress on Unmanned Systems Engineering*, Granada, Spain. 10.14323/ijuseng.2015.17

Al-Shibli, M. (2019). *Blockchain Artificial Intelligent Drone Network and Cloud System*, EFS ID: 34731423, Application Number 62787335. USPTO Patent.

Al-Shibli, M. (2019). *Blockchain Drone Satellite Network System (BlockchainDroneSatNet) and Cryptocurrency (Drone Satellite Coin: DSAC AND Drone Satellite Token: DSAT)*, EFS ID: 34737619, Application Number 62787531. USPTO Patent.

Al-Shibli, M. (2019). *Blockchain-Enabled Peer-to-Peer Drone Delivery Service*, EFS ID: 34727686, Application Number 62786800. USPTO Patent.

- Altbach, P. G., Gumport, P. J., & Berdahl, R. O. (Eds.). (2011). *American higher education in the twenty-first century* (3rd ed.). Baltimore, MD: The Johns Hopkins University Press.
- Altmann, S. P. (1903). Simmel's philosophy of money. *American Journal of Sociology*, 9(1), 46–68. doi:10.1086/211195
- Alvares, C. (2018). Online staging of femininity: Disciplining through public exposure in Brazilian social media. *Feminist Media Studies*, 1–18.
- Alvarez Technology Group. (2018). *2018 Top Cybercrime Facts and Why You Should Care*. Retrieved May 11, 2019, from <https://www.alvareztg.com/2018-cybercrime-statistics-reference-material/>
- Alvari, H., Shakarian, P., & Snyder, J. K. (2016, September). A non-parametric learning approach to identify online human trafficking. In *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on* (pp. 133-138). IEEE. 10.1109/ISI.2016.7745456
- Alvari, H., Shakarian, P., & Snyder, J. K. (2017). Semi-supervised learning for detecting human trafficking. *Security Informatics*, 6(1), 1. doi:10.1186/13388-017-0029-8
- Alzubaidi, A., & Kalita, J. (2015). Authentication of Smartphone Users Using Behavioral Biometrics. *Journal of IEEE Communications Surveys and Tutorials*.
- Amanda Project. (n.d.). *AMANDA Project - Virtual Reality Anti-Bullying App*. Author.
- Amarasekara, B. R., & Mathrani, A. (2016). *Controlling Risks and Fraud in Affiliate Marketing: A Simulation and Testing Environment*. PST2016 (Privacy, Security and Trust - IEEE 14th Annual Conference), Auckland, New Zealand.
- Amarasekara, B. R. (2017). *Analysis, design and simulation of fraud and vulnerability management in affiliate marketing: a thesis submitted to the Massey University of Auckland in fulfilment of the requirements for the degree of Master of Philosophy, Massey University of Auckland*. Auckland, New Zealand: Massey University. Retrieved from <http://hdl.handle.net/10179/12128>
- Amazon. (2018). *Alexa - Amazon Devices - Amazon Official Site*. Retrieved from Amazon Official Site: <https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011>
- Ambika, P. (2018). Machine Learning. In P. Raj & A. Raman (Eds.), *Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science* (pp. 209–230). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-5972-6.ch011
- American Convention on Human Rights American Convention on Human Rights, opened for signature Nov. 22, 1969, 1144 UNTS 123, art. 13 (entered into force July 18, 1978).
- American National Standards Institute (2001). *Public-Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*. American National Standard X9.63.
- American National Standards Institute (2005). *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standard X9.62.
- Amin, S. (2010, January). *A Step Towards Modeling and Destabilizing Human Trafficking Networks Using Machine Learning Methods*. Paper presented at the AAAI Spring Symposium, Stanford, CA. Retrieved from <http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1155>
- Amossy, R. (2010). *La présentation de soi. Ethos et identité verbale*. Paris: PUF.
- Amsterdam, J. von. (2018). *Monero versus Bitcoin: The battle of the cryptocurrencies* (vol. 4). Academic Press.
- An attack on internet privacy. (2017, March 28). *The New York Times*, p. A26.

Compilation of References

- Ananthakrishnan, U., Li, B., & Smith, M. (2015). *A tangled web: Evaluating the impact of displaying fraudulent reviews*. Academic Press.
- Anderle, M. (2016). Making a More Empathetic Facebook - The company's compassion department researches ways to make confrontations and breakups a little easier online. *The Atlantic – Technology*.
- Anderson, J., & Rainie, L. (2017). *The future of truth and misinformation online*. Pew Research Center, Internet and Technology. Retrieved from <http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/>
- Anderson, M., & Jiang, J. (2018). *Teens, Social Media & Technology 2018*. Pew Research Center. Retrieved from <http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>
- Anderson, R. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy*. Berlin: Springer. doi:10.1007/978-3-642-39498-0_12
- Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., & Savage, S. (2012). Measuring the cost of cybercrime. *Proceedings of Workshop on Economics of Information Security (WEIS 2012)*, 1-31.
- Anderson, T. W., & Hsiao, C. (1982). Formulation and estimation of dynamic models using panel data. *Journal of Econometrics*, 18(1), 47–82. doi:10.1016/0304-4076(82)90095-1
- Andolina, S., Klouche, K., Ruotsalo, T., Floréen, P., & Jacucci, G. (2018). Querytogether: Enabling entity-centric exploration in multi-device collaborative search. *Information Processing & Management*, 54(6), 1182–1202. doi:10.1016/j.ipm.2018.04.005
- Angeli, G., Premkumar, M. J. J., & Manning, C. D. (2015). Leveraging linguistic structure for open domain information extraction. In *Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing* (Vol. 1, pp. 344-354). 10.3115/v1/P15-1034
- Ang, R. P. (2016). Cyberbullying: Its prevention and intervention strategies. In D. Sibnath (Ed.), *Child safety, welfare and well-being: Issues and challenges* (pp. 25–38). New York: Springer. doi:10.1007/978-81-322-2425-9_3
- Angwin, J., Mattu, S., & Parris, T., Jr. (2016, December 27). Facebook doesn't tell users everything it really knows about them. *ProPublica*. Retrieved from <https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>
- Anonym. (n.d.). *Binary newsgroups*. Retrieved from <http://www.usenetguide.de/Usenet/BinaryGroups.htm>
- Anonymous. (2006). XBOX 360 hacked to run Linux. *26th Chaos Communication Congr*. Retrieved from <http://www.youtube.com/watch?v=4AGAohJuovY>
- Anonymous. (2010, January). Keeping online customers. *Dealerscope*, 52(1), 26. Retrieved from <https://search-proquest-com.ezproxy.jyu.fi/docview/218956873?accountid=11774>
- Anonymous. (2016). Hacktivist groups can provide accountability. *USA Today*, 144(2853), 5-6.
- Anstead, M. (2000). *Taking a tough line on privacy*. Marketing.
- Antal, M., Szabo, L. Z., & László, I. (2015). Keystroke dynamics on Android platform. *Procedia Technology*, 19, 820–826. doi:10.1016/j.protcy.2015.02.118
- Antoniades, D., Markatos, E. P., & Dovrolis, C. (2009). One-click hosting services: a file-sharing hideout. In *Proceedings of the 9th acm sigcomm conference on internet measurement* (pp. 223–234). 10.1145/1644893.1644920

- Antonius, N., & Rich, L. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The International Technology Management Review*, 3(1), 42–53. doi:10.2991/itmtr.2013.3.1.4
- Antonopoulos, A.M. (2014). *Mastering Bitcoin, Unlocking digital crypto-currencies*. O'Reilly Media, Inc.
- Antonopoulos, A. M. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media, Inc.
- Aoyama, I., Utsumi, S., & Hasegawa, M. (2011). Cyberbullying in Japan: Cases, government reports, adolescent relational aggression and parental monitoring roles. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Bullying in the global playground: Research from an international perspective*. Oxford, UK: Wiley-Blackwell.
- Appazov, A. (2014). *Legal Aspects of Cybersecurity*. Copenhagen: Justitministeriet Denmark. Retrieved January 11, 2019, from http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf
- APWG (Anti-phishing Working Group). (2018). Phishing Activity Trends Report, 2nd Quarter 2018. Retrieved from <https://www.apwg.org/resources/apwg-reports/>
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. doi:10.1089/cyber.2010.0307 PMID:22007957
- Aribake, F. O. (2015). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A conceptual Review. *International Journal of Trade, Economics and Finance*, 6(5), 272–277. doi:10.18178/ijtef.2015.6.5.481
- Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *Cyberpsychology & Behavior*, 11(3), 253–261. doi:10.1089/cpb.2007.0016 PMID:18537493
- Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, 54(1), 46–56. doi:10.1080/01930826.2014.893116
- ARM. (2009). *Security technology building a secure system using TrustZone™ technology* (white paper). ARM Limited.
- Armerding, T. (2015). *Cybercrime: Much more organized*. CSO, IDG Communications, Inc. Retrieved from <https://www.csoonline.com/article/2938529/cyber-attacks-espionage/cybercrime-much-more-organized.html>
- Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141–165. doi:10.1080/01495939308402915
- Arroyo-Gallego, T., Ledesma-Carbayo, M. J., Sánchez-Ferro, A., Butterworth, I., Mendoza, C. S., Matarazzo, M., & Giancardo, L. (2017). Detection of Motor Impairment in Parkinson's Disease via Mobile Touchscreen Typing. *IEEE Transactions on Biomedical Engineering*, 64(9), 1994–2002. doi:10.1109/TBME.2017.2664802 PMID:28237917
- Arslan, S., Savaser, S., Hallett, V., & Balci, S. (2012). Cyberbullying among primary school students in Turkey: Self-reported prevalence and associations with home and school life. *Cyberpsychology, Behavior, and Social Networking*, 15(10), 527–533. doi:10.1089/cyber.2012.0207 PMID:23002988
- Asenas, J.J. & Hubble, B.R. (2018). Trolling Free Speech Rallies: Social Media Practices and the (Un)Democratic Spectacle of Dissent. *Taboo*, 17(2), 36-53. doi:10.31390/taboo.17.2.06
- Ashiq, J. (2015, April 30). The Importance of cyber hygiene in cyberspace. *Infosec Institute*. Retrieved from <http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace/#gref>

Compilation of References

- Asko, D. (2017). *Cyberhate on cyber space: cyberbullying – A new phenomenon of violence among youth*. Council of Europe.
- Aslan, D. (2011). Critically evaluating typologies of internet sex offenders: A psychological perspective. *Journal of Forensic Psychology Practice*, 11(5), 406–431. doi:10.1080/15228932.2011.588925
- AsSadhan, B., Moura, J.M.F., & Lapsley, D. (2009). Periodic Behavior in Botnet Command and Control Channels Traffic. *Proceedings of the IEEE Global Telecommunications Conference*, 1-6.
- Astinova, M. (2013). *The Crime of Child Pornography: European Legislative and Police Cooperation Initiatives* (Master Thesis). Tilburg University.
- Astolfi, F., Kroese, J., & Van Oorschot, J. (2015). *I2P - The Invisible Internet Project*. Academic Press.
- Astolfi, F., Kroese, J., & van Oorschot, J. (2015). *I2p-the invisible internet project*. Media Technology, Leiden University, Web Technology Report.
- Atabekova, A., & Filippov, V. (2018). Legislation Response to Use of Minors' Self-generated Sexual Content for their ICT-facilitated Sexual Coercion. *European Research Studies Journal*, 21(4), 763–772.
- Atherton, K. D. (2015, May). When virtual crimes get prosecuted in real life. A dungeon dive into Diablo's in-game crime spree. *Popular Science*. Retrieved from <http://www.popsoci.com/no-sanctuary-diablos-game-thieves>
- Atroszko, P., Balcerowska, J., Bereznowski, P., Biernatowska, A., Pallesen, S., & Andressen, C. (2018). Facebook addiction among Polish undergraduate students: Validity of measurement and relationship with personality and well-being. *Computers in Human Behavior*, 85, 329–338. doi:10.1016/j.chb.2018.04.001
- Atton, C., & Hamilton, J. (2008). Theorizing alternative journalism. In *Journalism Studies: Key Texts: Alternative journalism* (pp. 117–135). London: SAGE Publications Ltd. doi:10.4135/9781446216163.n8
- Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. *6th International Conference on Principles of Security and Trust (POST), European Joint Conferences on Theory and Practice of Software*. 10.1007/978-3-662-54455-6_8
- Atzei, N., Bartoletti, M., & Cimoli, T. (2018). SoK: unraveling Bitcoin smart contracts. *7th International Conference on Principles of Security and Trust (POST), European Joint Conferences on Theory and Practice of Software*.
- Aubrey, S. M. (2004). *The new dimension of international terrorism*. Zurich: vdf Hochschulverlag AG.
- Augenstein, S. (2017). NYC truck terror attack: New 'lone wolf' study may help analysis. *PoliceOne News*. Retrieved from <https://www.policeone.com/investigations/articles/455533006-NYC-truck-terrorattack-New-lone-wolf-study-may-help-analysis/>
- August, M. B. (2016). *The Red Zone: Russian conflict management in the Gray Zone* (Doctoral dissertation, Sciences).
- Australian Government. (2012, September 12). *Cybercrime Legislation Act120(2012). An Act to implement the Council of Europe Convention on Cybercrime, and for other purposes*. Retrieved October 30, 2018, from <https://www.legislation.gov.au/Details/C2012A00120>
- Avasthi, S., & Sanwal, T. (2016). Biometric Authentication Techniques: A Study on Keystroke Dynamics. *International Journal of Scientific Engineering and Applied Science*, 2(1), 215–221.
- Averbuch, A., Kiperberg, M., & Zaidenberg, N. J. (2011, September). An efficient vm-based software protection. In *2011 5th International Conference on Network and System Security* (pp. 121-128). IEEE. 10.1109/ICNSS.2011.6059968

- Avgerinos, T. B., Brumley, D., Davis, J., Goulden, R., Nighswander, T., Rebert, A., & Williamson, N. (2018). The Mayhem Cyber Reasoning System. *IEEE Security and Privacy*, 16(2), 52–60. doi:10.1109/MSP.2018.1870873
- Aviles, G. (2015). *How U.S. political and socio-economic trends promotes hacktivist activity* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses.
- Awadi, H. R. A., & Belaton, B. (2015). Multi-phase IRC Botnetand Botnet Behavior Detection Model. *ArXiv e-prints*.
- Awan, I., & Zempi, I. (2016). The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts. *Aggression and Violent Behavior*, 27, 1–8.
- Awofeso, N. (2017). Improving efficiency and reducing fraud in UAE's health insurance market. *Journal of Financial Markets*, 1(1), 7–16. Retrieved from <http://www.alliedacademies.org/articles/improving-efficiency-and-reducing-fraud-in-uaes-health-insurance-market.pdf>
- Ayas, T., & Horzum, M. B. (2010). *Cyberbullg / victim scale development study*. Retrieved from: <http://www.akademik-bakis.org>
- Aydın, A. O. (2013). *Yapay Zekâ: Bütünleşik Biliş Doğru*. İstanbul: İstanbul Gelişim Üniversitesi Yayınları.
- Ayedun, C. A., Durodola, O. D., & Akinjare, O. A. (2012). An Empirical Ascertainment of the Causes of Building Filure and Collapse in Nigeria. *Mediterranean Journal of Social Sciences*, 3(1), 313–323.
- Ayedun, C.A., Durodola, O. D., Oni, S. A., Oluwatobi, A.O., & Ikotun, O.T. (2018). The Flooding Effect on Residential Property Values: A Case Study of Shogunro Residential Estate, Agege; Lagos State Nigeria. *International Journal of Civil Engineering and Technology*, 9(6), 489–496.
- Ayenson, M., Wambach, D., Soltani, A., Good, N., & Hoofnagle, C. (2011). *Flash Cookies And Privacy II: Now with HTML5 and ETag Respawning*. World Wide Web Internet and Web Information Systems.
- Ayofe, A. N., & Osunade, O. (2009). Towards Ameliorating Cybercrime and Cybersecurity. *International Journal of Computer Science and Information Security*, 3(1), 1–11.
- Azeem, M. (2018, October 03). FIA allowed to open 15 centres to check cybercrime. *Dawn*. Retrieved from <https://www.dawn.com/news/1436438>
- Babaeizadeh, M., Bakhtiari, M., & Maarof, M. A. (2014). Keystroke Dynamic Authentication in Mobile Cloud Computing. *International Journal of Computer Applications*, 90, 29–36.
- Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior*, 44(1), 45–66. doi:10.1007/s10508-014-0270-x PMID:24627189
- Baccarella, C., Wagner, T., Kietzmann, J., & McCarthy, I. (2018). Social media? It's serious! Understanding the dark side of social media. *European Management Journal*, 36(4), 431–438. doi:10.1016/j.emj.2018.07.002
- Bachore, M. M. (2016). The nature, causes and practices of academic dishonesty/cheating in higher education: The case of Hawassa University. *Journal of Education and Practice*, 7(19), 14–20.
- Bacık, G. (2005). Kamusal Alan Tanımı Üzerine Bir Tartışma. In A. Erol (Ed.), *Sivil Bir Kamusal Alan* (pp. 9–17). İstanbul: Kaknüs Yayınevi.
- Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B., & Gosling, S. D. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological Science*, 21(3), 372–374. doi:10.1177/0956797609360756 PMID:20424071

Compilation of References

- Baecher, P., Koetter, M., Holz, T., Dornseif, M., & Freiling, F. C. (2006). The nepenthes platform: An efficient approach to collect malware. *Lecture Notes in Computer Science*, 4219, 165–184.
- Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74–94. doi:10.1007/BF02723327
- Bahnsen, A. C., Torroledo, I., Camacho, L. D., & Villegas, S. (2018). DeepPhish: Simulating Malicious AI. *Black Hat Europe*. Retrieved from https://albahnsen.com/wp-content/uploads/2018/05/deepphish-simulating-malicious-ai_submitted.pdf
- Bai, G., Jiang, J., & Flasher, R. (2017). Hospital Risk of Data Breaches. *JAMA Internal Medicine*, 177(6), 878. doi:10.1001/jamainternmed.2017.0336 PMID:28384777
- Bailey, M. (2018). U.S. Policy on Human Trafficking, A Partial Solution for a Perplexing Global Human Rights Problem. *Indonesian Journal of International & Comparative Law*, (4), 607. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.indjic15.30&site=eds-live>
- Bailey, E., Rice, S., Robinson, J., Nedeljkovic, M., & Alvarez-Jimenez, M. (2018). Theoretical and empirical foundations of a novel online social networking intervention for youth suicide prevention: A conceptual review. *Journal of Affective Disorders*, 238, 499–505. doi:10.1016/j.jad.2018.06.028 PMID:29936387
- Baker, P. (2001). Moral panic and alternative identity construction in Usenet. *Journal of Computer-Mediated Communication*, 7(1).
- Baker, A., Addario, L., Winters, P., & Rhodan, M. (2019). The Survivor. *Time*, 193(3), 36. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edb&AN=134160312&site=eds-live>
- Balbín, C. (2011). *Tratado de Derecho Administrativo*. Buenos Aires: La Ley.
- Balduzzi, M., & Ciancaglini, V. (2015). *Cybercrime in the Deep Web Black Hat EU*. Amsterdam: Trend Micro.
- Balestra, R. (1988). *Manual de Derecho Internacional Privado*. Buenos Aires: Abeledo Perrot.
- Ballard, A. M., Cardwell, T., & Young, A. M. (2019). Fraud detection protocol for web-based research among men who have sex with men: Development and descriptive evaluation. *JMIR Public Health and Surveillance*, 5(1), e12344. doi:10.2196/12344 PMID:30714944
- Bandyopadhyay, S. (2011). Antecedents And Consequences Of Consumers Online Privacy Concerns. *Journal of Business & Economics Research*, 7(3). doi:10.19030/jber.v7i3.2269
- Banerjee, A., Faloutsos, M., & Bhuyan, L. (2007). The p2p war: Someone is monitoring your activities! In *International conference on research in networking* (pp. 1096–1107). Academic Press.
- Banerjee, S. P., & Woodard, D. L. (2012). Biometric Authentication and Identification using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research*, 7(1), 116–139. doi:10.13176/11.427
- Banet-Weiser, S., & Miltner, K. M. (2016). # MasculinitySoFragile: Culture, Structure, and Networked Misogyny. *Feminist Media Studies*, 16(1), 171–174. doi:10.1080/14680777.2016.1120490
- Banistar, D. (2006). *Freedom of information around the World*. Retrieved 18 March 2017, from http://www.humanright-sinitiative.org/propagams/ai/international/laws_paper/intl/gobal_foi_surbey_2006.pdf
- Bank, J. (2010). Regulating Hate Speech Online. *International Review of Law, Computers & Technology*, 3, 235.

- Bankole, F. O., & Bankole, O. O. (2017). The effects of cultural dimension on ICT innovation: Empirical analysis of mobile phone services. *Telematics and Informatics*, 34(2), 490–505. doi:10.1016/j.tele.2016.08.004
- Banks, D., & Kyckelhahn, T. (2011). *Characteristics of suspected human trafficking incidents, 2008-2010*. U.S. Department of Justice. Retrieved from <http://bjs.ojp.usdoj.gov/content/pub/pdf/cshti0810.pdf>
- Banks, W. C. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory Law Review*, 66(3), 513–525.
- Banu, M. Z., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies*, 4(6), 783–786.
- Barabási, A. (2012). *Network science*. Boston, MA: Barabási Lab.
- Baradaran, N., & Habibi, H. (2017). Cyber Warfare and Self-Defense from the Perspective of International Law. *J. Pol. & L.*, 10, 40.
- Baravalle, A., Lopez, M. S., & Lee, S. W. (2016, December). Mining the dark web: drugs and fake IDs. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)* (pp. 350-356). IEEE. 10.1109/ICDMW.2016.0056
- Barboza, D. (2005, December). Ogre to slay? Outsource it to Chinese. *The New York Times*. Retrieved from <http://www.nytimes.com/2005/12/09/technology/ogre-to-slay-outsource-it-to-chinese.html>
- Barford, P., & Yegneswaran, V. (2007). An inside look at botnets. In *Malware detection* (pp. 171–191). Boston, MA: Springer. doi:10.1007/978-0-387-44599-1_8
- Bar-Hillel, Y. (1951). The present state of research on mechanical translation. *American Documentation*, 2(4), 229–237. doi:10.1002/asi.5090020408
- Bar-Hillel, Y. (1953). Some linguistic problems connected with machine translation. *Philosophy of Science*, 20(3), 217–225. doi:10.1086/287266
- Barlett, C. P., & Gentile, D. A. (2012). Long-term psychological predictors of cyber-bullying in late adolescence. *Psychology of Popular Media Culture*, 2, 123–135. doi:10.1037/a0028113
- Barlett, C. P., Gentile, D. A., Anderson, C. A., Suzuki, K., Sakamoto, A., Yamaoka, A., & Katsura, R. (2013). Cross-cultural differences in cyberbullying behavior: A short-term longitudinal study. *Journal of Cross-Cultural Psychology*, 45(2), 300–313. doi:10.1177/0022022113504622
- Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Retrieved from <https://www.eff.org/cyberspace-independence>
- Barnett, S. (2016). Top 10 challenges to securing a network. *Network Security*, 2000(1), 14–16. doi:10.1016/S1353-4858(00)86652-0
- Barney, D. (2018). Trafficking Technology: A Look at Different Approaches to Ending Technology-Facilitated Human Trafficking. *Pepperdine Law Review*, (4), 747. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.pepplr45.25&site=eds-live>
- Baroni, D. (2015, July 3). New Zealand Government To Punish Online Trolls With Prison Time. Retrieved from <http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time>
- Barrat, J. (2013). *Our Final Invention: Artificial Intelligence and the End of the Human Era*. Thomas Dunne Books.
- Barratt, M. J., & Maddox, A. (2018). Dark Web. *The SAGE Encyclopedia of the Internet*.

Compilation of References

- Barrett, M. J., & Ferris, J. A. (2014). *Use of Silk Road, the online drug marketplace, in the United Kingdom* (5th ed., Vol. 109). Australia and the United States: Society for the Study of Addiction; doi:10.1111/add.12470
- Barrio, P., & Gravano, L. (2017). Sampling strategies for information extraction over the deep web. *Information Processing & Management*, 53(2), 309–331. doi:10.1016/j.ipm.2016.11.006
- Barroso, P. (2001) Cyberspace: Ethical problems with new technology. *Ethicomp*.
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. doi:10.1016/j.tele.2017.04.013
- Bartlett, J. (2015). *The dark net : Inside the digital underworld*. Academic Press.
- Bartlett-Bragg, A. (2006). *Reflections on pedagogy: Reframing practice to foster informal learning with social software*. Retrieved from: <http://www.dream.sdu.dk/uploads/files/Anne%20Bartlett-Bragg.pdf>
- Bartlett, J., & Miller, C. (2013). *The state of the art: A literature review of social media intelligence capabilities for counter-terrorism*. London: DEMOS.
- Bärtl, M. (2018). YouTube channels, uploads and views: A statistical analysis of the past 10 years. *Convergence (London)*, 24(1), 16–32. doi:10.1177/1354856517736979
- Barton, L., & Walker, S. (2007). The conflict perspective: A Marxian approach. In R. Meighan & C. Harber (Eds.), *A sociology of educating* (5th ed.; pp. 316–335). New York: Continuum International Publishing Group.
- Baryshnikov, M. (2016). *Jailhouse hypervisor* (Bachelor's thesis). České vysoké učení technické v Praze. Vypočetní a informační centrum.
- Baskerville, R. (2008). What design science is not. *European Journal of Information Systems*, 17(5), 441–443. doi:10.1057/ejis.2008.45
- Bastiaenssens, S., Vandeboosch, H., Poels, K., Van Cleemput, K., DeSmet, A., & De Bourdeaudhuij, I. (2014). Cyberbullying on social network sites. An experimental study into bystanders' behavioural intentions to help the victim or reinforce the bully. *Computer. Human Behavior*, 31, 259–271. doi:10.1016/j.chb.2013.10.036
- Basu, I. (2011). Security and development—are they two sides of the same coin? Investigating India's two-pronged policy towards Left Wing extremism. *Contemporary South Asia*, 19(4), 373–393. doi:10.1080/09584935.2010.537745
- Baudrillard, J. (1994). *Simulacra and Simulation* (S. F. Glaser, Trans.). Ann Arbor, MI: University of Michigan Press.
- Bauman, S., Underwood, M.K., & Card, N.A (2013). Definitions: Another perspective and a proposal for beginning with cyberaggression. *Principles of cyberbullying research: Definitions, measures, and methodology*, 41–46.
- Baumann, A., Haupt, J., Gebert, F., & Lessmann, S. (2018). The Price of Privacy: An Evaluation of the Economic Value of Collecting Clickstream Data. *Business & Information Systems Engineering*, 1–19. doi:10.1007/12599-018-0528-2
- Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence*, 36(2), 341–350. doi:10.1016/j.adolescence.2012.12.001 PMID:23332116
- Bauman, S., Underwood, M. K., & Card, N. A. (2013). Definitions: Another perspective and a proposal for beginning with cyberaggression. In S. Bauman, D. Cross, & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, methodology* (pp. 26–40). New York, NY: Routledge.
- Bauman, Z. (1997). *Modernite ve Holocaust*. İstanbul: Sarmal Yayınevi.

- Bauman, Z. (2003). *Comunidad. En busca de seguridad en un mundo hostil*. Madrid: Siglo XXI.
- Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 2(8), 121–144. doi:10.1111/ips.12048
- Bayar, Y., & Ucanok, Z. (2012). School social climate and generalized peer perception in traditional and cyberbullying status. *Educational Sciences: Theory and Practice*, 12, 2352–2358.
- Beale, A., & Hall, K. (2007). Cyberbullying: What school administrators (and parents) can do. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, 81(1), 8–12. doi:10.3200/TCHS.81.1.8-12
- Bech, J. (2014). *OP-TEE, open-source security for the mass-market*. Core Dump.
- Beckman, L., Hagquist, C., & Hellstrom, L. (2012). Does the association with psychosomatic health problems differ between cyberbullying and traditional bullying? *Emotional & Behavioural Difficulties*, 17(3-4), 421–434. doi:10.1080/13632752.2012.704228
- Beebe, S., Beebe, S., & Redmond, M. (2005). *Interpersonal communication: Relating to others* (5th ed.). Boston: Pearson.
- Behzadan, V., Munir, A., & Yampolskiy, R. V. (2018). A Psychopathological Approach to Safety Engineering in AI and AGI. In *Computer Safety, Reliability, and Security. SAFECOMP 2018*. Cham: Springer. doi:10.1007/978-3-319-99229-7_46
- Beinatt, S., Anderson, B., Lee, S., & Utting, D. (2002). *Youth at risk? A national survey of risk factors, protective factors and problem behaviours among young people in England, Scotland and Wales*. London: Community That Cares.
- Belch, G. E., & Belch, M. A. (2009). Source, message, and channel factors. In *Advertising & promotion: An integrated marketing communications perspective* (8th ed.; pp. 174–205). Boston: McGraw-Hill Irwin.
- Bell, D., & Blanchflower, D. (2010). *Young people and Recession: a lost generation*. Working paper. Dartmouth College.
- Bellamy, A., & Williams, P. (2010). Understanding Peacekeeping. *Polity*.
- Bellamy, A., & Williams, P. (2013). *Providing Peacekeepers: The Politics, Challenges, and Future of United Nations Peacekeeping Contributions*. OUP. doi:10.1093/acprof:oso/9780199672820.001.0001
- Bellare, M., & Rogaway, P. (1993, August). Entity authentication and key distribution. In *Annual international cryptology conference* (pp. 232-249). Springer.
- Bellovin, S. (2001). Security aspects of napster and gnutella. In *2001 USENIX annual technical conference*. USENIX.
- Belsey, B. (2004). *Cyberbullying.ca*. Retrieved July 31, 2004, from Web site: www.cyberbullying.ca
- Ben Yehuda, R., & Zaidenberg, N. J. (2018). Hyplets - Multi Exception Level Kernel towards Linux RTOS. *Proceedings of the 11th ACM International Systems and Storage Conference Systor 2018*, 116-117.
- Benediktova, B., & Nevosad, L. (2008). *Affiliate Marketing - Perspective of content providers*. Department of Business Administration and Social Sciences. Lulea University of Technology.
- Bennell, C., & Jones, N. J. (2005). Between a ROC and a Hard Place: A Method for Linking Serial Burglaries by Modus Operandi. *Journal of Investigative Psychology and Offender Profiling*, 2(1), 23–41. doi:10.1002/jip.21
- Bennett, M. (2017). Building a digital security army. *The Telegraph*. Retrieved from <https://www.telegraph.co.uk/business/digital-security/human-behaviour-in-digital-security/>
- Bennett, R. R. (1991). Routine activities: A cross-national assessment of a criminological perspective. *Social Forces*, 70(1), 147–163. doi:10.2307/2580066

Compilation of References

- Benson, V., Saridakis, G., & Tennakoon, H. (2015c). Purpose of social networking use and victimisation: are there any differences between university students and those not in HE? *Computers in Human Behavior*, 51(B), 867-872.
- Benson, V. (2017). *The State of Global Cyber Security: Highlights and Key Findings*. London, UK: LT Inc. doi:10.13140/RG.2.2.22825.49761
- Bergman, M. K. (2001). White paper: the deep web: surfacing hidden value. *The Journal of Electronic Publishing: JEP*, 7(1). doi:10.3998/3336451.0007.104
- Bergstrom, A. (2013). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419-426. doi: 0747-5632/ doi:10.1016/j.chb.2015.07.025
- Berkeley, U. C. (2018). Phishing Examples Archive. Retrieved from <https://security.berkeley.edu/resources/phishing/phishing-examples-archive>
- Berliner, H. J. (1980). Backgammon Computer Program Beats World Champion. *Artificial Intelligence*, 14(2), 205-220. doi:10.1016/0004-3702(80)90041-7
- Berners-Lee, T., Dimitroyannis, D., Mallinckrodt, A. J., & McKay, S. (1994). World Wide Web. *Computers in Physics*, 8(3), 298-299. doi:10.1063/1.4823300
- Bernstein v. United States Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999)
- Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1996 U.S. Dist. LEXIS 5084, 96 D.A.R. 6721 (N.D. Cal. 1996)
- Berry, B. (2004). Organizational Culture: A Framework and Strategies for Facilitating Employee Whistleblowing. *Employee Responsibilities and Rights Journal*, 16(1), 1-11. doi:10.1023/B:ERRJ.0000017516.40437.b1
- Bertrand, N. (2019, April 19). 5 Unresolved Mysteries about Russian Meddling in Mueller's Report. *Politico*. Retrieved from <https://www.politico.com/story/2019/04/19/mueller-mysteries-1283775>
- Besarabov, Z. & Kolev, T. (2018). *Predicting digital asset market based on blockchain activity data*. International Science and Engineering Fair.
- Bhasin, D. M. (2016, Feb.). The fight against bank frauds: Current scenario and future challenges. *Ciência e Técnica Vitivinícola*.
- Bhaskar, V., Linacre, R., & Machin, S. (2017, November 6). *Dark web: The economics of online drugs markets*. Retrieved from LSE Business Review: <http://blogs.lse.ac.uk/businessreview/2017/11/06/dark-web-the-economics-of-online-drugs-markets/>
- Bhatti, B. M., & Sami, N. (2015). Building adaptive defense against cybercrimes using real-time data mining. *2015 First International Conference on Anti-Cybercrime (ICACC)*. 10.1109/Anti-Cybercrime.2015.7351949
- Bhutani, N., Jagadish, H. V., & Radev, D. (2016). Nested propositions in open information extraction. In *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing* (pp. 55-64). 10.18653/v1/D16-1006
- Bi, W, Jia, X., Zheng, M. (2018). *A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain, Computer Science, Cryptography and Security*. arXiv.org.
- Biddle, P., England, P., Peinado, M., & Willman, B. (2003). The darknet and the future of content protection. In J. Feigenbaum (Ed.), *Digital rights management* (pp. 155-176). Berlin: Springer Berlin Heidelberg. doi:10.1007/978-3-540-44993-5_10

Bidgoli, H. (Ed.). (2009). *Global perspectives in information security: legal, social and international issues*. Hoboken, NJ: J. Wiley & Sons.

Biere, S. (2018). *Hate speech detection using natural language processing techniques*. Vrije Universiteit Amsterdam. Retrieved from https://beta.vu.nl/nl/Images/werkstuk-biere_tcm235-893877.pdf

Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010). On the analysis of the zeus botnet crimeware toolkit. In *Privacy Security and Trust (PST). Eighth Annual International Conference*, 31–38.

Biocca, S., Feldstein De Cardenas, S., & Basz, V. (1997). *Lecciones de Derecho Internacional Privado*. Buenos Aires, Ed. Universidad.

Biryukov, A., Pustogarov, I., Thill, F., & Weinmann, R.-P. (2014). Content and popularity analysis of tor hidden services. In *2014 IEEE 34th international conference on distributed computing systems workshops (icdcs)* (pp. 188–193). IEEE. 10.1109/ICDCSW.2014.20

Biryukov, A., & Pustogarov, I. (2015, May). Bitcoin over Tor isn't a Good Idea. In *2015 IEEE Symposium on Security and Privacy* (pp. 122-134). IEEE. 10.1109/SP.2015.15

Bischoff, P. (2018, September 12). Step by step guise to safely accessing the dark net and deep web. *VPN & Privacy*. Retrieved from <https://www.comparitech.com/blog/vpn-privacy/how-to-access-the-deep-web-and-darknet/#gref>

Bischoff, P. (2018, September 6). *Analysis: How data breaches affect stock market share prices*. Retrieved August 19, 2018, from <https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/>

Bisson, D. (2015). *5 Social Engineering Attacks to Watch Out For*. Retrieved December 6, 2018, from <https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>

Biswas, B., Pal, S., & Mukhopadhyay, A. (2016). *AVICS-Eco framework: An approach to attack prediction and vulnerability assessment in a cyber Ecosystem*. Academic Press.

Bitcoin. (n.d.). Retrieved from <https://bitcoin.org/en/>

Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse & Neglect*, 44, 140–149. doi:10.1016/j.chiabu.2014.12.004 PMID:25613089

Blanzieri, E., & Bryl, A. (2008). A survey of learning-based techniques of email spam filtering. *Artificial Intelligence Review*, 29(1), 63–92. doi:10.1007/10462-009-9109-6

Blau, A. (2017, December 11). Better cybersecurity starts with fixing your employees' bad habits. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits>

Block, W. (2000). Threats, blackmail, extortion, and other bad things. *Tulsa Law Review*, 35(2), 333-351. Retrieved from <https://digitalcommons.law.utulsa.edu/cgi/viewcontent.cgi?article=2218&context=tlr>

blockgeeks.com. (2018a). *A Deeper Look at Different Smart Contract Platforms*. Retrieved from <https://blockgeeks.com/guides/different-smart-contract-platforms>

blockgeeks.com. (2018b). *How to Audit a Smart Contract*. Retrieved from <https://blockgeeks.com/guides/audit-smart-contract/>

Blond, S. L., Manils, P., Abdelberi, C., K^aafar, M. A., Castelluccia, C., Legout, A., & Dabbous, W. (2011). *One bad apple spoils the bunch: Exploiting P2P applications to trace and profile tor users*. Retrieved from <http://arxiv.org/abs/1103.1518>

Compilation of References

- Bloomberg. (2018, September 11). *How Faking Videos Became Easy -- And Why That's So Scary*. Retrieved from <http://fortune.com/2018/09/11/deep-fakes-obama-video/>
- Blue Ridge Thunder. (2018). *How Online Predators Work*. Retrieved from <https://www.blueridgethunder.com/how-online-predators-work/>
- Blum, S. D. (2009, February 20). Academic integrity and student plagiarism: A question of education, not ethics. *The Chronicle of Higher Education*, 55(24), A35.
- Blundell, R., & Bond, S. (1998). Initial conditions and moment restrictions in dynamic panel data models. *Journal of Econometrics*, 87(1), 115–143. doi:10.1016/S0304-4076(98)00009-8
- Blundell, R., & Bond, S. (2000). GMM estimation with persistent panel data: An application to production functions. *Econometric Reviews*, 19(3), 321–340. doi:10.1080/07474930008800475
- Boakye, O. M., & Marfo, Y. M. (2016). Utilizing Keystroke Dynamics as an Additional Security Measure to Password Security in Computer Web-based Applications - A Case Study of UEW. *International Journal of Computers and Applications*, 149(5), 35–44. doi:10.5120/ijca2016911402
- Boardhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8(1), 1–20. Retrieved from <http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf>
- Boateng, R. (2014). Resources, electronic-commerce capabilities and electronic-commerce benefits: Conceptualizing the links. *Information Technology for Development*, 22(2), 242–264. doi:10.1080/02681102.2014.939606
- Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa-cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, 11(2), 85–100.
- Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family*. Westport, CT: Praeger.
- Bocij, P. (2006). *The dark side of Internet: Protecting Yourself and your Family from Online Criminals*. Westport, CT: Praeger Pubischer.
- Bock, B. C., Marcus, B. H., Pinto, B. M., & Forsyth, L. H. (2001). Maintenance of physical activity following an individualized motivationally tailored intervention. *Annals of Behavioral Medicine*, 23(2), 79–87. doi:10.1207/S15324796ABM2302_2 PMID:11394558
- Boden, E. (2018). *How hackers infiltrate healthcare organizations* | eSentire. Retrieved from <https://www.esentire.com/blog/healthcare-cyber-attack-types/>
- Bodine-Baron, E., Helmus, T., Radin, A., & Treyger, E. (2018). *Countering Russian Social Media Influence*. RAND Cooperation. Retrieved from https://www.rand.org/pubs/research_reports/RR2740.html
- Bohannon, J. (2016, March 9). Why criminals can't hide behind Bitcoin. *Science*. doi:10.1126/science.aaf4167
- Bollacker, K., Evans, C., Paritosh, P., Sturge, T., & Taylor, J. (2008, June). Freebase: a collaboratively created graph database for structuring human knowledge. In *Proceedings of the 2008 ACM SIGMOD international conference on Management of data* (pp. 1247-1250). ACM. 10.1145/1376616.1376746
- Bolsin, S., Pal, R., Wilmschurst, P., & Pena, M. (2011). Whistleblowing and patient safety: The patient's or the profession's interests at stake? *Journal of the Royal Society of Medicine*, 104(7), 278–282. doi:10.1258/jrsm.2011.110034 PMID:21725092

- Bonanno, R. A., & Hymel, S. (2013). Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying. *Journal of Youth and Adolescence*, 42(5), 685–697. doi:10.1007/10964-013-9937-1 PMID:23512485
- Bondada, M. B., & Bhanu, S. M. S. (2014). Analyzing User Behavior Using Keystroke Dynamics to Protect Cloud from Malicious Insiders. *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 1-8. 10.1109/CCEM.2014.7015481
- Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In *Annual international cryptography conference* (pp. 213-229). Springer. 10.1007/3-540-44647-8_13
- Boniface, K. A., & Michael, K. A. (2014). Curbing Cybercrime by Application of Internet Users' Identification System (IUIS) in Nigeria, *World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering*, 8(9), 1582–1585.
- Bonilla, H. (2018, April 20). Dark Web breaches can affect your compliance with GDPR. *SWK Network Services*. Retrieved from <https://www.swknetworkservices.com/dark-web-breaches-compliance-gdpr/>
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Research perspectives and challenges for bitcoin and cryptocurrencies (extended version). *Cryptology ePrint Archive, Report 2015/452*.
- Bontrager, P., Roy, A., Togelius, J., Memon, N., & Ross, A. (2018). *DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution*. eprint arXiv:1705.07386
- Booth, R. E. (2017). The Effect of Freedom of Expression and Access to Information on the Relationship between ICTs and the Well-being of Nations. *Proceedings of the 23rd Americas Conference on Information Systems*.
- Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach to evaluating risk of targeted violence. *Behavioral Sciences & the Law*, 17(3), 323–337. doi:10.1002/(SICI)1099-0798(199907/09)17:3<323::AID-BSL349>3.0.CO;2-G PMID:10481132
- Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014). Elliptic Curve Cryptography in Practice, Financial Cryptography and Data Security. *18th International Conference, Revised Selected Papers, FC 2014*, Christ Church, Barbados.
- Bostrom, N. (2014). *Superintelligence*. Oxford, UK: Oxford University Press.
- Bosworth, K., Espelage, D., & Simon, T. (1999). Factors associated with bullying behavior among early adolescents. *The Journal of Early Adolescence*, 19(3), 341–362. doi:10.1177/0272431699019003003
- Bouche, V. (2015). A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims. *Thorn Foundation*. Retrieved from https://www.wearethorn.org/wpcontent/uploads/2015/02/Survivor_Survey_r5.pdf
- Boud, D., Cohen, R., & Walker, D. (1993). Using experience for learning. Bristol, PA: The Editors and Contributors.
- Boulton, M., Lloyd, J., Down, J., & Marx, H. (2012). Predicting undergraduates' self-reported engagement in traditional and cyberbullying from attitudes. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 141–147. doi:10.1089/cyber.2011.0369 PMID:22304402
- Bourdieu, P. (1976). *Entwurf einer Theorie der Praxis auf der ethnologischen Grundlage der kabyliischen Gesellschaft*. Frankfurt am Main: Suhrkamp.
- Bourdieu, P. (1984). *Distinction: A social critique of the judgement of taste*. Cambridge, MA: Harvard University Press.

Compilation of References

- Bove, V., & Elia, L. (2011). Supplying peace: Participation in and troop contribution to peacekeeping missions. *Journal of Peace Research*, 48(6), 699–714. doi:10.1177/0022343311418265
- Bowles, N. (2018, June 23). Thermostats, locks and lights: Digital tools of domestic abuse. *New York Times*. Retrieved from <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>
- Bowles, M. (2012). The business of hacking and birth of an industry. *Bell Labs Technical Journal*, 17(3), 5–16. doi:10.1002/bltj.21555
- Bowman-Grieve, L. (2009). Exploring “Stormfront”: A virtual community of radical right. *Studies in Conflict and Terrorism*, 32(11), 989–1007. doi:10.1080/10576100903259951
- Boyd, D., Casteel, H., Thakor, M., & Johnson, R. S. (2011). *Human trafficking and technology: A framework for understanding the role of technology in the commercial exploitation of children in the US*. Microsoft Research.
- Boyd, M., & Ellison, B. (2007). Social Network Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 201–230. doi:10.1111/j.1083-6101.2007.00393.x
- Brackbill, H. (1929). Some Telegraphers’ Terms. *American Speech*, 4(4), 287–290. doi:10.2307/452061
- Bradbury, D. (2014). Unveiling the dark web. *Network Security*, 2014(4), 14–17. doi:10.1016/S1353-4858(14)70042-X
- Bradshaw, T., & Cookson, R. (2011, February 7). Hactivist group in switch to securities. *The Financial Times*, p. 15.
- Brambilla, M., Ceri, S., & Halevy, A. (2013). Special issue on structured and crowd-sourced data on the Web. *The VLDB Journal*, 22(5), 587–588. doi:10.1007/00778-013-0327-9
- Brandimarte, L., Acquisti, A., & Lowenstein, G. (2013). Misplaced confidences, privacy, and the control paradox. *Social Psychological & Personality Science*, 4(3), 340–347. doi:10.1177/1948550612455931
- Branigan, S. (2011, July 31). Revenge Hacking. Retrieved May 17, 2019, from Trends in high tech security website: <https://sbranigan.wordpress.com/2011/07/31/revenge-hacking/>
- Brantlinger, E. (2007). (Re) Turning to Marx to understand the unexpected anger among “winners” in schooling: A critical social psychological perspective. In *Late to class: Social class and schooling in the new economy*. Albany, NY: State University of New York Press.
- Brantly, A. (2017). Banning Encryption to Stop Terrorists: A Worse than Futile Exercise. *CTC Sentinel*, 10, 7.
- Brear, D., & Barnes, S. J. (2008). Assessing the value of online affiliate marketing in the UK financial services industry. *International Journal of Electronic Finance*. doi:10.1504/IJEF.2008.016881
- Breiding, M. J., Basile, K. C., Smith, S. G., Black, M. C., & Mahendra, R. R. (2015). *Intimate partner violence surveillance: Uniform definitions and recommended data elements, Version 2.0*. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.
- Breitbarth, A. K., Morgan, J., & Jones, A. L. (2018). E-cigarettes—An unintended illicit drug delivery system. *Drug and Alcohol Dependence*, 192, 98–111.
- Brenner, S. (2001). *International law enforcement*. Retrieved October 21, 2018, from <http://www.cybercrimes.net/International/LawEnforcement.html>
- Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, CA: Praeger.
- Brenner, S. W. (2004). U.S. Cybercrime Law: Defining Offenses. *Information Systems Frontiers*, 6(2), 115–132. doi:10.1023/B:ISFI.0000025780.94350.79

- Brenner, S. W. (2010). *Cybercrime. Criminal Threats from Cyberspace*. Santa Barbara, CA: Greenwood Publishing Group.
- Brenner, S. W. (2014). *Cyberthreats and the decline of the nation-state*. Routledge. doi:10.4324/9780203709207
- Brewer, G., & Kerslake, J. (2015). Cyberbullying, self-esteem, empathy and loneliness. *Computers in Human Behavior*, 48, 255–260. doi:10.1016/j.chb.2015.01.073
- Brewster, T. (2018, March 13). This insane map shows all of the beauty and horror of the Dark Web. *Forbes*. Retrieved from <https://www.forbes.com/sites/thomasbrewster/2018/03/13/dark-web-map-6000-webpages/#2f26b53018e7>
- Brewster, T. (2016, July 25). Who's Better At Phishing Twitter, Me Or Artificial. *Forbes*.
- Brey, P. (1999). The Ethics of Representation and Action in Virtual Reality. *Ethics and Information Technology*, 1(1), 5–14. doi:10.1023/A:1010069907461
- Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: Has the internet enabled a new typology of sex offender? *Sexual Abuse*, 23(1), 72–91. doi:10.1177/1079063210384275 PMID:20947699
- Brighi, A., Guarini, A., Melotti, G., Galli, S., & Genta, M. L. (2012). Predictors of victimisation across direct bullying, indirect bullying and cyberbullying. *Emotional & Behavioural Difficulties*, 17(3-4), 375–388. doi:10.1080/13632752.2012.704684
- Bright, L., & Logan, K. (2018). Is my fear of missing out (FOMO) causing fatigue? Advertising, social media fatigue, and the implications for consumers and brands. *Internet Research*, 28(5), 1213–1227. doi:10.1108/IntR-03-2017-0112
- British Computing Society. (2017, May). Demystifying the Dark Web. *British Computing Society*. Retrieved from <https://www.bcs.org/content/conWebDoc/57766>
- Broadband Commission for Digital Development. (2015). *Cyber violence against women and girls*. Retrieved 10th of October 2018 from <https://en.unesco.org/sites/default/files/genderreport2015final.pdf>
- Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., & Da, C. (2013). *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups*. Australian National University Cybercrime Observatory. Working Paper. Retrieved December 3, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2211842
- Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408–433. doi:10.1108/13639510610684674
- Broadrick v. Oklahoma, 413 US 601 (US, 1973).
- Broll, R. (2018). Cyberbullying: Four steps to protect your kids. *The Conversation*. Retrieved from <https://theconversation.com/cyberbullying-four-steps-to-protect-your-kids-90907>
- Bromium, & McGuire, M. (2018, April). *RSA Conference 2018*. Retrieved July 19, 2018, from <https://www.rsaconference.com/events/us18>
- Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., ... Dredze, M. (2018). Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *American Journal of Public Health*, 108(10), 1378–1384. doi:10.2105/AJPH.2018.304567 PMID:30138075
- Brooks, R. (2018). *Rule of Law in the Gray Zone*. Retrieved from <https://mwi.usma.edu/rule-law-gray-zone/>
- Brooks-Gunn, J., & Duncan, G. J. (2007). The effects of poverty on children. *The Future of Children*, 7, 34–39. PMID:9299837

Compilation of References

- Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Héту, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International*, 264, 7-14. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0379073816300676>
- Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International*, 277, 88-102. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0379073817302037>
- Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Héту, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International*, 264, 7-14. doi:10.1016/j.forsciint.2016.02.045 PMID:26978791
- Brown, B. (2001). *Studying the internet experience*. HP Laboratories Technical Report HPL-2001-49. Retrieved from <http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf>
- Brown, D. R. L. (2009). *Standards for Efficient Cryptography Group. SEC 1: Elliptic Curve Cryptography*. Certicom Corp. Research, Version 2.0.
- Brown, D. R. L. (2010). *SEC 2: Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography*. Certicom Corp. Research, Version 2.0.
- Brown, M. R. (2003). *Playstation 2 independence day*. Retrieved from http://www.ifcaro.net/PS2_Independence_Exploit/original.htm
- Brown, A., Slater, G., & Spencer, D. A. (2002). Driven to abstraction? Critical realism and the search for the 'inner connection' of social phenomena. *Cambridge Journal of Economics*, 26(6), 773-788. doi:10.1093/cje/26.6.773
- Brown, D. (2010). Resilient botnet command and control with tor. *DEF CON*, 18, 105.
- Brown, P., Halsey, A. H., Lauder, H., & Wells, A. S. (1997). The transformation of education and society: An introduction. In A. H. Halsey, H. Lauder, P. Brown, & A. S. Wells (Eds.), *Education: culture, economy, society*. Oxford, UK: Oxford University Press.
- Brown, S. E., Esbensen, F., & Geis, G. (2013). *Criminology: Explaining crime and its context* (8th ed.). Elsevier Inc.
- Brownson, H. L. (1953). Literature notes. *American Documentation*, 4(4), 174-184. doi:10.1002/asi.5090040406
- Bruchmann, K., Koopmann-Holm, B. & Scherer, A. (2018). Seeing Beyond Political Affiliations: The Mediating Role of Perceived Moral Foundations on the Partisan Similarity-Liking Effect. *PLoS One*, 13(8), 1-20. doi:10.1371/journal.pone.0202101
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., . . . Héigeartaigh, S. Ó. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute.
- Brunner, J. A. (2017). The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency. *Jurimetrics*, 57(3), 397-431. Retrieved from <https://search.proquest.com/docview/1965541412?accountid=10373>
- Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young people's online interactions. *Computers in Human Behavior*, 30, 299-306. doi:10.1016/j.chb.2013.09.012
- Bryk, A. (2018). *Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology*. Retrieved from <https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors>
- BT (British Telecom). (2017, Oct 17). *BT and Interpol Unite to Fight Cybercrime*. Retrieved from BT: <https://www.globalservices.bt.com/en/aboutus/news-press/bt-and-interpol-unite-to-fight-cybercrime>

- Buchan, R., & Tsagourias, N. (2016). Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence. *Journal of Conflict and Security Law*, 377-381. doi:10.1093/jcs/lkrw017
- Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys and Tutorials*, 18(2), 1153-1176. doi:10.1109/COMST.2015.2494502
- Building a Secure Future, One blockchain at a time.* (2018). US Senate Joint Economic Committee.
- Bullée, J. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks – A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, 15(1), 20-45. doi:10.1002/jip.1482
- Bullesbach, A. (2004). *Current challenges of data protection in the world economy*. Retrieved, September 30, 2018, from http://www.26konferencja.giodo.gov.pl/data/resources/BullesbachA_pres_en.pdf
- Bundaberg Hospital Commission of Inquiry Report. (2005). Retrieved from <https://www.casewatch.net/foreign/patel/interimreport.pdf>
- Buono, L. (2012). Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). *New Journal of European Criminal Law*, 4(3), 332-343. doi:10.1177/203228441200300307
- Burbano, D., & Hernandez-Alvarez, M. (2017, October). Identifying human trafficking patterns online. In *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6). IEEE.
- Burgess, M. (2016, December). Massive Yahoo database reportedly sold for £240,000 on the dark web. *Wired*. Retrieved from <https://www.wired.co.uk/article/yahoo-one-billion-accounts-hacked>
- Burgess, M. (2017, October). That Yahoo data breach actually hit three billion accounts. *Wired*. Retrieved from <https://www.wired.co.uk/article/hacks-data-breaches-2017>
- Burgess, J., & Green, J. (2018). *YouTube: Online Video and Participatory Culture*. Cambridge, UK: Polity.
- Burke Winkelman, S., Oomen-Early, J., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring cyber harassment among women who use social media. *Universal Journal of Public Health*, 3(5), 194-201. doi:10.13189/ujph.2015.030504
- Burke, J. (2019, August 11). Norway mosque attack suspect 'inspired by Christchurch and El Paso shootings'. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2019/aug/11/norway-mosque-attack-suspect-may-have-been-inspired-by-christchurch-and-el-paso-shootings>
- Burnap, P., French, R., Turner, F., & Jones, K. (2017). Malware classification using self organising feature maps and machine activity data. *Computers & Security*, 73, 399-410. doi:10.1016/j.cose.2017.11.016
- Burnier, D. (1994). Constructing political reality: Language, symbols, and meaning in politics: A review essay. *Political Research Quarterly*, 47(1), 239-253.
- Burrell, J. (2012). Producing the Internet and Development: an ethnography of Internet cafe use in Accra, Ghana. The London School of Economics and Political Science (LSE).
- Burrows, R. & Savage, M. (2014, April). After the crisis? Big data and the methodological challenges of empirical sociology. *Big Data & Society*, 1-6.
- Burstein, F. V., & Gregor, S. (1999). The systems development or engineering approach to research in information systems: An action research perspective. In *Proceedings of 10th Australasian Conference on Information Systems* (pp. 122-134). Academic Press.

Compilation of References

- Burton, K. A., Florell, D., & Wygant, D. B. (2013). The role of peer attachment and normative beliefs about aggression on traditional bullying and cyberbullying. *Psychology in the Schools*, 50(2), 103–114. doi:10.1002/pits.21663
- Bushing, Sven, & Marcan. (2010). Console hacking 2010: PS3 epic fail. *27th Chaos Communication Congr.*
- Buxton, J., & Bingham, T. (2015). The Rise and Challenge of Dark Net Drug Markets. *GDPO*.
- Bynum, T. W. (2000). *A very short history of Computer ethics*. Retrieved from http://www.southernct.edu.organizations/rccs/textonly/resources_t/research_t/introduction_t/bynum_shrt_hist_t.html
- C.M. (2018, May16). Impact of the Dark Web on cybersecurity and Internet governance. *DarkWebNews*. Retrieved from <https://darkwebnews.com/dark-web/impact-of-darkweb-in-cybersecurity-and-internet/>
- Cabinet Office. (2011). *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*. London: Crown.
- Cahill, T. P., Rozinov, K., & Mule, C. (2003, 6). Cyber warfare peacekeeping. In *Information Assurance Workshop*, 2003. *IEEE Systems, Man and Cybernetics Society*, (pp. 100-106). IEEE.
- California State University Sacramento. (2016). *Kantian ethics*. Retrieved from <http://www.csus.edu/indiv/g/gaskilld/ethics/kantian%20ethics.htm>
- Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security and Privacy*, 7(1), 78–81. doi:10.1109/MSP.2009.12
- Calvão, F. (2018). Crypto-miners: Digital labor and the power of blockchain technology. *Economic Anthropology*, 6(1), 123–134. doi:10.1002/ea.12136
- Camacho, D., Gilpérez-López, I., Gonzalez-Pardo, A., Ortigosa, A., & Urruela, C. (2016, November). *CEUR Workshop Proceedings*. Retrieved from <http://ceur-ws.org/Vol-1794/afcai16-paper5.pdf>
- Cameron, D. (2018). Privacy and Security. Identity theft is exploding in the developing countries. *Cybercrime*. Retrieved September 9, 2019, from, <https://gizmodo.com/identity-theft-is-exploding-in-developing-countries-1825745097>
- Cameron, D. (2018, September 11). Simple hack turns India's massive biometric database into a profitable counterfeit system. *Gizmodo*, Retrieved from <https://gizmodo.com/simple-hack-turns-indias-massive-biometric-database-int-1828972521>
- Cameron, A. C., & Trivedi, P. K. (2005). *Microeconometrics: methods and applications*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511811241
- Campbell, A. (1990). Female participation in gangs. In C. Ronald Huff (Ed.), *Gangs in America* (pp. 163–182). Newbury Park, CA: Sage Publications.
- Camp, J., & Lewis, K. (2001). Code as speech: A discussion of Bernstein v. USDOJ, Karn v. USDOS, and Junger v. Daley in light of the US Supreme Court's recent shift to Federalism. *Ethics and Information Technology*, 3(1), 21–33. doi:10.1023/A:1011427806551
- Canadian Nurses Association. (1999). *I see and I'm silent; I see and I speak out – the ethical dilemma of whistleblowing*. Retrieved from https://www.cna-aiic.ca/~media/cna/page-content/pdf-en/ethics_pract_see_silent_november_1999_e.pdf
- Canan, S., & Acungil, M. (2018). *Dijital Gelecekte İnsan Kalmak*. İstanbul: Tuti Kitap.
- Cao, J., Karras, P., Raïssi, C., & Tan, K.-L. (2010). p-uncertainty: Inference-proof transaction anonymization. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 3(1–2), 1033–1044. doi:10.14778/1920841.1920971

- Caplan, S. E. (2010). Theory and measurement of generalized problematic Internet use: A two-step approach. *Computers in Human Behavior*, 26(5), 1089–1097. doi:10.1016/j.chb.2010.03.012
- Cappadocia, M. C., Craig, W. M., & Pepler, D. (2013). Cyberbullying: Prevalence, stability and risk factors during adolescence. *Canadian Journal of School Psychology*, 28(2), 171–192. doi:10.1177/0829573513491212
- Capron, H. L. (Ed.). (1996). *Computers: tools for an information age*. The Benjamin/Cummings Publishing Company, Inc.
- Capurro, R. (2006). Towards an Ontological Foundation of Information Ethics. *Ethics and Information Technology*, 8(4), 175–186. Retrieved from <http://www.capurro.de/oxford.html>
- Carlini, N., & Wagner, D. (2018). *Audio Adversarial Examples: Targeted Attacks on Speech-to-Text*. arXiv:1801.01944
- Carminati, M., Polino, M., Continella, A., Lanzi, A., Maggi, F., & Zanero, S. (2018). Security Evaluation of a Banking Fraud Analysis System. *ACM Trans. Priv. Secur.*, 21(3). doi:10.1145/3178370
- Carpenter, N. (2018, December). South Korean law to punish boosters passes in the National Assembly. *Dot Esports*. Retrieved from <https://dotesports.com/overwatch/news/lucios-winter-wonderland-skin-turns-him-into-a-futuristic-snow-fox>
- Carpentier. (2016). *Online abuse: how different countries deal with it*. Retrieved 10th of October 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>
- Carr, D. (2008). How Obama Tapped Into Social Networks' Power. *The New York Times*. Available at <https://www.nytimes.com/2008/11/10/business/media/10carr.html>
- Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc.
- Carr, N. (2010). *The Shallows: what the internet is doing to our brains*. New York, NY: W. W. Norton & Company.
- Carter, D. L. (1995). Computer Crime Categories. *Law Enforcement Bulletin, U. S. Department of Justice. Federal Bureau of Investigation*, 64(7), 21–26.
- Carter, J. A., Maher, S., & Neumann, P. R. (2014). *Greenbirds: Measuring importance and influence in Syrian Foreign fighter networks*. London: ICSR.
- Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5), 545–547. doi:10.1188/14.ONF.545-547 PMID:25158659
- Cartwright, B. E. (2016). Cyberbulling and Cyber Law. A Canadian Perspective. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-7. Retrieved May 15, 2019, from <https://ieeexplore.ieee.org/document/7740430/citations>
- Carver, C. (2014). *E-fencing detection: mining online classified ad websites for stolen property* (Doctoral dissertation).
- Casale, S., & Fioravanti, G. (2018). Why narcissists are at risk for developing Facebook addiction: The need to be admired and the need to belong. *Addictive Behaviors*, 76, 312–318. doi:10.1016/j.addbeh.2017.08.038 PMID:28889060
- Casey, E. (2008). Cyberpatterns: Criminal Behavior on the Internet. In B. E. Turvey (Ed.), *Criminal profiling: An introduction to behavioral evidence analysis* (3rd ed.). London: Academic Press.
- Caspi, A., Wright, B. R., Moffitt, T. E., & Silva, P. A. (1998). Early failure in the labour market: Childhood and adolescent predictors of unemployment in the transition to adulthood. *American Sociological Review*, 63(3), 424–451. doi:10.2307/2657557
- Cassagne, J. (2007). *Tratado de Derecho Procesal Administrativo*. Buenos Aires: La Ley.

Compilation of References

- Cassese, A. (2005). *International Law*. Oxford, UK: Oxford University.
- Cassidy, P. (2017, November 3). Man petrol bombed homes in revenge for Facebook post. STV News. Retrieved from <https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/>
- Castaldo, L., & Cinque, V. (2018, February). Blockchain-based logging for the cross-border exchange of ehealth data in europe. In *International ISCIS Security Workshop* (pp. 46-56). Springer. 10.1007/978-3-319-95189-8_5
- Castells, M. (2001). *Internet y la sociedad red*. Academic Press.
- Castells, M. (1997). *The End of the Millennium, the Information Age: Economy, Society and Culture* (Vol. 3). Cambridge: MA: Blackwell.
- Castoriadis, C. (1975). *L'institution imaginaire de la société*. Paris: Seuil.
- Castro, D. (2013). How much will PRISM cost the US cloud computing industry? *The Information Technology & Innovation Foundation*, 1-9.
- Castronova, E. (2008). *Synthetic Worlds*. University of Chicago Press.
- Cattapan, T. (2000). Destroying e-commerce's "cookie monster" image. *Direct Marketing*, 62(12), 20–24.
- Cavalier, R. (2002). *Online guide to ethics and moral philosophy: Utilitarian theories*. Retrieved from <http://caae.phil.cmu.edu/Cavalier/80130/part2/sect9.html>
- Cayoglu, U. (2014). *Report: The Process Model Matching Contest 2013*. In *BPM 2013: Business Process Management Workshops* (pp. 442–463). Springer.
- CBS News. (2016). Retrieved from <https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/>
- CEDAW. (1992). *General Recommendation No. 19*. Retrieved 10th of October 2018 from <http://www.refworld.org/docid/52d920c54.html>
- CEDAW. (2017). *General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19*. Retrieved 10th of October 2018 from https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf
- Cenkseven Önder, F., & Yurtal, F. (2008). An Investigation of the Family Characteristics of Bullies, Victims, and Positively Behaving Adolescents. *Educational Sciences: Theory and Practice*, 8(3), 821–832.
- Center for Internet Security. (2018). *Data Breaches: In the Healthcare Sector*. Retrieved from <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/>
- Center for Strategic and International Studies. (2017). Assessing the Third Offset Strategy. *CSIS*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170302_Ellman_ThirdOffsetStrategySummary_Web.pdf?EX01GwjFU22_Bkd5A.nx.fJXTKRDKbVR
- Ceyhan, E. (2013). Kişilik Gelişimi. In G. Can (Ed.), *Eğitim Psikolojisi* (pp. 82–112). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.
- Chaabane, A., Manils, P., & Kaafar, M. A. (2010). Digging into anonymous traffic: A deep analysis of the tor anonymizing network. In *2010 fourth international conference on network and system security* (pp. 167–174). 10.1109/NSS.2010.47

Chachra, N., McCoy, D., Savage, S., & Voelker, J. M. (2014). Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting. *Proceedings of the Workshop on the Economics of Information Security (WEIS)*. Retrieved from <https://cseweb.ucsd.edu/~voelker/pubs/namevalue-weis14.pdf>

Chachra, N., Savage, S., & Voelker, G. (2015). Affiliate Crookies: Characterizing Affiliate Marketing Abuse. In *IMC '15 Proceedings of the 2015 ACM Conference on Internet Measurement Conference* (pp. 41-47). New York, NY: ACM. doi:10.1145/2815675.2815720

Chachra, N. (2015). *Understanding URL Abuse for Profit*. San Diego, CA: University of California.

Chae, J. (2018). Reexamining the relationship between social media and happiness: The effect of various social media platforms on reconceptualized happiness. *Telematics and Informatics*, 35(6), 1656–1664. doi:10.1016/j.tele.2018.04.011

Chainalysis. (2018). *The changing nature of cryptocrime*. Retrieved from https://www.chainalysis.com/static/Cryptocrime_Report_V2.pdf

Chai, W. (2019). Threat assessment of violent extremism: Considerations and applications. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 53–72). Singapore: World Scientific Press.

Chalk, A. (2016, December). Creating hacks for online games could now earn you jail time in South Korea. *PCGamer*. Retrieved from <http://www.pcgamer.com/south-korea-makes-cheating-in-online-games-an-actual-crime/>

Chandel, A., Kumar, P., & Yadav, D. K. (2017). Phishing attacks and countermeasures. *International Journals of Advanced Research in Computer Science and Software Engineering*, 7(6), 246–253. doi:10.23956/ijarcsse/V7I6/0227

Chang, C.C., & Lin, C.J. (2011). LIBSVM: A Library for Support Vector Machines. *ACM Transactions on Intelligent Systems and Technology*, 2(3).

Chang, C. C., Yan, C. F., & Tseng, J. S. (2012). Perceived convenience in an extended technology acceptance model: Mobile technology and English learning for college students. *Australasian Journal of Educational Technology*, 28(5). doi:10.14742/ajet.818

Chang, C. H., Kaye, M., Girgis, M. R., & Shaalan, K. F. (2006). A survey of web information extraction systems. *IEEE Transactions on Knowledge and Data Engineering*, 18(10), 1411–1428. doi:10.1109/TKDE.2006.152

Chang, C. L. (2011). The Effect of an Information Ethics Course on the Information Ethics Values of Students—A Chinese guanxi culture perspective. *Computers in Human Behavior*, 27(5), 2028–2038. doi:10.1016/j.chb.2011.05.010

Chapman, A. (2001). La propiedad intelectual como derecho humano. *Boletín de Derechos de Autor*.

Charaudeau, P. (2017). *Le débat public. Entre controverse et polémique. Enjeu de vérité, enjeu de pouvoir*. Limoges: Lambert-Lucas.

Charlesworth, J. (2018, September 10). *AI can produce pictures, but can it create art for itself?* Retrieved from CNN News: <https://www.cnn.com/style/article/artificial-intelligence-ai-art/index.html>

Charter of the United Nations. (1945). Retrieved from <http://www.un.org/en/sections/un-charter/un-charter-full-text/>

Chatterjee, J. (n.d.). IoT with Big Data Framework using Machine Learning Approach. *International Journal of Machine Learning and Networked Collaborative Engineering*, 2(2), 75-85.

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, 10(1), 247–256. doi:10.14257/ijasia.2016.10.1.23

Compilation of References

- Chaum, D. (2003). Untraceable electronic mail, return addresses and digital pseudonyms. In *Secure electronic voting* (pp. 211–219). Boston, MA: Springer. doi:10.1007/978-1-4615-0239-5_14
- Chavez, N., & Holcombe, M. (2019, March 17). Death toll rises to 50 in New Zealand mosque shootings. *CNN*. Retrieved from <https://edition.cnn.com/2019/03/16/asia/christchurch-new-zealand-mosque-shooting-latest/index.html>
- Chawki, M. (2009). Nigeria Tackles Advance Free Fraud. *Journal of Information, Law & Technology*, 1, 1-20. Retrieved from http://go.warwick.ac.uk/jilt/2009_1/chawki
- Chen, X., Tan, J., Goh, P., Ong, G., & Khader, M. (2018). *Frequently asked questions about fake news* (HTBSC Research Report S02/2018). Singapore: Home Team Behavioural Sciences Centre.
- Chen, Y. C., Li, Y. J., Tseng, A., & Lin, T. (2017, October). Deep learning for malicious flow detection. In *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on* (pp. 1-7). IEEE. 10.1109/PIMRC.2017.8292316
- Cheng, F., & Evans, E. (2012). *U.S. Patent Application No. 13/447,986*. Washington, DC: US Patent Office.
- Cheng, Z. Y., Liu, Y., Chang, C. C., & Guo, C. (2013). A fault-tolerant group key agreement protocol exploiting dynamic setting. *International Journal of Communication Systems*, 26(2), 259–275. doi:10.1002/dac.2506
- Chen, H. (2011). *Dark web: Exploring and data mining the dark side of the web* (Vol. 30). Springer Science & Business Media.
- Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291–302. doi:10.1016/j.chb.2017.01.003
- Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American Society for Information Science and Technology*, 59(8), 1347–1359. doi:10.1002/asi.20838
- Chen, X. K. (2018). Fake News After a Terror Attack: Psychological Vulnerabilities Exploited by Fake News Creators. In M. Khader, L. S. Neo, D. D. Cheong, & J. Chin (Eds.), *Learning from Violent Extremist Attacks: Behavioural Sciences Insights for practitioners and policymakers* (pp. 435–451). World Scientific Press. doi:10.1142/9789813275447_0023
- Chen, X., Tan, J., Goh, P., Ong, G., & Khader, M. (2018). *Frequently Asked Questions about Fake News* [HTBSC Research Report S02/2018]. Singapore: Home Team Behavioural Sciences Centre.
- Chen, Y., YekkehZaare, I., & Zhang, A.F. (2018). Real or bogus: Predicting susceptibility to phishing with economic experiments. *PLoS One*, 13(6). doi:10.1371/journal.pone.0198213
- Chen, Y., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management & Data Systems*, 107(1), 21–36. doi:10.1108/02635570710719034
- Chen, Y.-H., Hsu, I.-C., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of Business Research*, 63(9–10), 1007–1014. doi:10.1016/j.jbusres.2009.01.023
- Cherneko, E., Demidov, O., & Lukyanov, F. (2018). *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*. Council on Foreign Relations. Retrieved December 2, 2018, from <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms>
- Chertoff, M., & Simon, T. (2015). *The impact of the Dark Web on Internet governance and cyber security*. Retrieve Oct 2, 2018 from https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

- Chertoff, M. (2017). A Public Policy Perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), 26–38. doi:10.1080/23738871.2017.1298643
- Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107.
- Chideya, F. (2015). *Medical Privacy Under Threat in the Age of Big Data*. Retrieved from <https://theintercept.com/2015/08/06/how-medical-privacy-laws-leave-patient-data-exposed/>
- Chiu, M. M., Siegfried-Spellar, K., & Ringenberg, T. (2018). Exploring detection of contact vs. fantasy online sexual offenders in chats with minors: Statistical discourse analysis of self-disclosure and emotion words. *Child Abuse & Neglect*, 81, 28–138. doi:10.1016/j.chiabu.2018.04.004 PMID:29730313
- Cho, Y., & Newhouse, D. (2011). *How did the great recession affect different types of workers? Evidence from 17 middle income countries*. Policy research working paper 5636. Washington, DC.: World Bank
- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 8, 42–51. doi:10.1016/j.chb.2017.12.001
- Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1).
- Choo, B., Dillon, L., Neo, L. S., Ong, G., Tan, E., & Khader, M. (2016). *Social engineering: Using psychology to exploit bugs in the human operation system (HTBSC Research Report No.: 01/2016)*. Singapore: Ministry of Home Affairs, Home Team Behavioural Sciences Centre.
- Choo, K. K. R. (2005). Revisit Of McCullagh-Barreto Two-Party ID-Based Authenticated Key Agreement Protocols. *International Journal of Network Security*, 1(3), 154–160.
- Chothia, F.-S. T., Chothia, T., & Chatzikokolakis, K. (n.d.). A survey of anonymous peer-to-peer. In Proceedings of the IFIP international symposium on network-centric ubiquitous systems (ncus 2005). Springer.
- Chothia, T., Cova, M., Novakovic, C., & Toro, C. G. (2012). The unbearable lightness of monitoring: Direct monitoring in bittorrent. In *International conference on security and privacy in communication systems* (pp. 185–202). Academic Press.
- Chou, T. (2016). *Precision: Principles, Practices and Solutions for the Internet of Things*. Morrisville, NC: Lulu.com.
- Chourci, N. (2012). *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press.
- Christina, G. (2012). #mencallmethings: 'FUCKIN HOE,' 'FUCKIN FEMINAZI SLUT.'" *Greta Christina's Blog: Atheism, sex, politics, dreams, and whatever*, August 8. Retrieved 10th of October 2018 <https://the-orbit.net/greta/2012/08/27/mencallmethings-old-bag/>
- ChristopherN. (2018). Retrieved from ETRise: <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/hackers-mined-a-fortune-from-indian-websites/articleshow/65836088.cms>
- Chu, B. (2017, October 9). What is 'nudge theory' and why should we care? Explaining Richard Thaler's Nobel economics prize-winning concept. *Independent*. Retrieved from <https://www.independent.co.uk/news/business/analysis-and-features/nudge-theory-richard-thaler-meaning-explanation-what-is-it-nobel-economics-prize-winner-2017-a7990461.html>
- Chun, R. (2018, April). China's new frontiers in dystopian tech. *The Atlantic*. Retrieved from <https://www.theatlantic.com/magazine/archive/2018/04/big-in-china-machines-that-scan-your-face/554075/>
- Chung, W., & Paynter, J. (2002). Privacy Issues on the Internet. *Proceedings of the 35th Hawaii International Conference on System Sciences*. 10.1109/HICSS.2002.994191

Compilation of References

- Ciaccia, C. (2018, July). Mobile games are being used for money laundering, report warns. *Fox News*. Retrieved from <https://www.foxnews.com/tech/mobile-games-are-being-used-for-money-laundering-report-warns>
- Ciampaglia, G., Shiralkar, P., Rocha, L., Bollen, J., Menzer, F., & Flammini, A. (2015). Computational Fact Checking from Knowledge Networks. *PLoS One*, 10(6), e0128193. doi:10.1371/journal.pone.0128193 PMID:26083336
- Ciancaglini, V., Balduzzi, M., McArdle, R., & Rösler, M. (2015). *Below the Surface: Exploring the deep Web*. Trend Micro. Retrieved November 28, 2018, from https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. doi:10.6028/NIST.SP.800-61r2
- Cimpanu, C. (2016, October). Online gaming currencies used to launder money for cyber-criminals. *Softpedia News*. Retrieved from <http://news.softpedia.com/news/online-gaming-currencies-used-to-launder-money-for-cyber-criminals-509177.shtml>
- Citron, D. K. (2009). Cyber civil rights. *BUL Rev.*, 89, 61–125.
- Clancy, C. M., Farquhar, M. B., & Sharp, B. A. (2005). Patient safety in nursing practice. *Journal of Nursing Care Quality*, 20(3), 193–197. doi:10.1097/00001786-200507000-00001 PMID:15965381
- Clarifying Lawful Overseas Use of Data Act (CLOUD) (2018). Pub. L. No. 115-141, 132 Stat. 348.
- Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. (2001). Freenet: A distributed anonymous information storage and retrieval system. In *Designing privacy enhancing technologies* (pp. 46–66). doi:10.1007/3-540-44702-4_4
- Clifford, C. (2018, August 7). *How billion-dollar start-up Darktrace is fighting cybercrime with A.I.* Retrieved from CNBC News: <https://www.cnbc.com/2018/08/07/billion-dollar-start-up-darktrace-is-fighting-cybercrime-with-ai.html>
- Clogston, J.F. (2016). The Repeal of the Fairness Doctrine and the Irony of Talk Radio: A Story of Political Entrepreneurship, Risk, and Cover. *Journal of Policy History*, 28(2), 375-396. doi:10.1017/S0898030616000105
- Clough, R. (2018). *The Inevitability of AI Law & Policy: Preparing Government for the Era of Autonomous Machines*. Public Knowledge. Retrieved from <https://www.publicknowledge.org/documents/the-inevitability-of-ai-law-policy-preparing-government-for-the-era-of-autonomous-machines/>
- Clough, J. (2015). *Principles of Cybercrime*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9781139540803
- Cockton, G. (2004). From quality in Use to Value in the World. In *Proceedings of the CHI'04 Extended Abstracts on Human factors in Computing Systems (CHI'04)*. New York: ACM Press. 10.1145/985921.986045
- COFACE – Confederation of Family Organisations in the European Union (2016). COFACE Paper – Cyberbullying, New dimensions through virtual environments and other emerging platforms and trends. *Coface-EU*.
- Coffey, A. (2001). *Education and social change*. Buckingham, UK: Open University Press.
- Coffey, K., Smith, R., Maglaras, L., & Janicke, H. (2018). Vulnerability Analysis of Network Scanning on SCADA Systems. *Security and Communication Networks*, 2018, 1–21. doi:10.1155/2018/3794603
- Cohen, B. (2003, May). *Incentives build robustness in bittorrent*. Retrieved from <http://bittorrent.org/bittorrentecon.pdf>
- Cohen, K. (2012). Who will be a lone wolf terrorist? Mechanisms of self-radicalisation and the possibility of detecting lone offender threats on the internet. Swedish Defence Research Agency (FOI).

- Cohen, M. C. (2007). *Responding to the barriers to academic success for local international students as an avenue to student success and to the internationalization of a community college* (Order No. 3252965). Available from ProQuest Dissertations & Theses Global. (304734360). Retrieved from <http://search.proquest.com.ezproxylocal.library.nova.edu/docview/304734360?accountid=6579>
- Cohen, A. K. (1955). *Delinquent boys*. Glencoe, IL: Free Press.
- Cohen-Almagor, R. (2018). Social responsibility on the Internet: Addressing the challenge of cyberbullying. *Aggression and Violent Behavior*, 39, 42–52. doi:10.1016/j.avb.2018.01.001
- Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20(1), 37–46. doi:10.1177/001316446002000104
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting linguistic markers for radical violence in social media. *Terrorism and Political Violence*, 26(1), 246–256. doi:10.1080/09546553.2014.849948
- Cohen, L. E., & Felson, M. (1979). On estimating the social costs of national economic policy: A critical examination of the Brenner study. *Social Indicators Research*, 6(2), 251–259. doi:10.1007/BF00343977
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. doi:10.2307/2094589
- Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2017, April). A formal security analysis of the signal messaging protocol. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on* (pp. 451-466). IEEE. 10.1109/EuroSP.2017.27
- Cole, G. F., Smith, C. E., & DeJong, C. (2018). *The American System Of Criminal Justice* (16th ed.). Boston, MA: Cengage.
- Coleman, J. (2012, August 30). Take ownership of your actions by taking responsibility. *Harvard Business Review*. Retrieved from <https://hbr.org/2012/08/take-ownership-of-your-actions>
- Coleman, E. G. (2014). *Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous*. London: Verso.
- Collinsdictionary.com. (2018). *Misandry definition and meaning* | Collins English Dictionary. Available at: <https://www.collinsdictionary.com/dictionary/english/misandry>
- Collister, S. (2014). Abstract hacktivism as a model for postanarchist organizing. *Ephemera: Theory & Politics in Organization*, 14(4), 765–779.
- Commission, E. U. (2018). What are my rights? *European Commission Policies, information and services*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en
- Computer Security Institute. (2001). *CSI/FBI 2001 Computer Crime and Security Survey*. Retrieved December 3, 2018, from <https://www.stealth-iss.com/documents/pdf/COMPSECSURVEY1.pdf>
- Concer, J., Paynich, R., & Gingerich, T. (2013). *Law enforcement in the United States*. Burlington, MA: Jones & Bartlett Learning.
- Conesa, P. (2018). *Hollywar: Hollywood, arme de propagande massive*. Paris: Robert Laffont.
- Conklin, J. E. (2007). *Criminology* (9th ed.). Pearson Education Inc.
- Connell, M., & Vogler, S. (2017). *Russia's approach to cyber warfare*. Center for Naval Analyses Arlington United States.

Compilation of References

Conroy, N., Rubin, V., & Chen, Y. (2016). Fake News or truth? Using satirical cues to detect potentially misleading news. *Proceedings Of the 2nd Workshop on Computational Approaches to Deception Detection*, 7-17.

Conspiracy to Commit Offense or to defraud United States 18 U.S.C. § 371

Consumer Pulse, C. M. B. (2015). *The Future of the Mobile Wallet: Barriers and opportunities for the next stage of the mobile payment revolution*. Retrieved from https://www.cmbinfo.com/assets/PR_Consumer-Pulse_MW_2015-min.pdf

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31–38. doi:10.19101/IJACR.2016.623006

Conway, M. (2007). Terrorist use of the Internet and the challenges of governing cyberspace. In D., Myriam, V., Mauer, & F., Krishna-Hensel (Eds.), *Power and security in the information age: Investigating the role of the state in cyberspace* (pp. 95-127). London: Ashgate.

Cook, M. (2016, May). Why online video gaming will be the next industry under cyber attack. *Information Week. IT Network*. Retrieved from <http://www.darkreading.com/vulnerabilities---threats/why-online-video-gaming-will-be-the-next-industry-under-cyber-attack-/a/d-id/1325519>

Cook, M. (2017, January). What to expect – Video game cybersecurity in 2017. *Gamasutra*. Retrieved from http://www.gamasutra.com/blogs/MatthewCook/20170112/289076/What_To_Expect__Video_Game_Cybersecurity_In_2017.php

Cook, T. (2018, October 24). *Keynote address from Tim Cook, CEO, Apple Inc.* Retrieved from <https://www.youtube.com/watch?v=kVhOLkIs20A>

Cooke, E., & Jahanian, F. (2005). The zombie roundup: Understanding, detecting, and disrupting botnets. In D. Katabi & B. Krishnamurthy (Eds.), *SRUTI. USENIX Association*.

Cooper, A. K. (2000, July 12). China: Government punishes Internet journalists. Committee to Protect Journalists. Retrieved from <https://cpj.org/2000/07/china-government-punishes-internet-journalists.php>

Cooper, E., & Chikada, A. (2015). *The Deep Web, the Darknet, and Bitcoin*. MarkMonitor - Part of Thomson Reuters. Retrieved November 28, 2018, from <https://www.markmonitor.com/download/webinar/2015/MarkMonitor-Webinar-150715-DeepWebDarknetBitcoin.pdf>

Corcoran, L., Connolly, I., & O'Moore, M. (2012). Cyberbullying in Irish schools: An investigation of personality and self-concept. *The Irish Journal of Psychology*, 33(4), 153–165. doi:10.1080/03033910.2012.677995

Corcoran, L., Mc Guckin, C., & Prentice, G. (2015). Cyberbullying or Cyber Aggression?: A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression. *Societies (Basel, Switzerland)*, 5(2), 245–255. doi:10.3390/soci5020245

Cormac, R. & Aldrich, R. J. (2018). Grey is the New Black: Covert Action and Implausible Deniability. *International Affairs*, 94(3), 477-494. doi:10.1093/ia/iyy067

Cormode, G., & Krishnamurthy, B. (2008). Key differences between Web 1.0 and Web 2.0. *First Monday*, 13(6). doi:10.5210/fm.v13i6.2125

Corse, A. (2018, September 18). The Cyberthreat's that most worry election officials. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/the-cyberthreats-that-most-worry-election-officials-1537322820>

Cortes, C., & Vapnik, V. (1995). Support-Vector Networks. *Machine Learning*, 20(3), 273–297. doi:10.1007/BF00994018

Cottam, R. W., & Gallucci, G. (1978). *The Rehabilitation of Power in International Relations: A Working Paper*. Pittsburgh, PA: University of Center for International Studies, University of Pittsburgh.

Cottam, M. L., & Cottam, R. W. (2001). *Nationalism and Politics: The Political Behavior of Nation States*. Boulder, CO: Lynne Reinner.

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

Council of Europe - Convention on Cybercrime. (2001). Retrieved July 19, 2018, from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_7_conv_budapest_en.pdf

Council of Europe. (2001). *Convention on Cybercrime*. Retrieved from coe.int/Treaty/en/Treaties/Html/185.htm

Council of Europe. (2001). *ETS 185 - Convention on Cybercrime, 23.XI.2001*. Retrieved May 15, 2019, from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_7_conv_budapest_en.pdf

Council of Europe. (2016). *Combating sexist hate speech*. Retrieved 10th of October 2018 from <https://edoc.coe.int/en/genderequality/6995-combating-sexist-hate-speech.html>

Council of Europe. (2016). *Training seminar countering hate speech through human rights education and narratives*. Retrieved from <https://rm.coe.int/16806efc97>

Council of Europe. (2018) *CyberCrime Convention Committee, Working Group on cyber bullying and other forms of online violence, especially against women and children (CBG), "Mapping study on cyber violence" (Draft)*. Retrieved 10th of October 2018 <https://rm.coe.int/t-cy-2017-10-cbg-study/16808b72da>

Council of Europe. (2018, March 19). *T-CY Drafting Group*. Retrieved from Council of Europe: <https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713>

Council on Foreign Relations. (2012). *U.S. Education Reform and National Security*. Council on Foreign Relations Press. Retrieved from <https://www.cfr.org/report/us-education-reform-and-national-security>

Cowie, I. (2009). *History does not repeat itself, but it often rhymes, as Mark Twain noted*. Retrieved from <https://www.telegraph.co.uk/finance/personalfinance/comment/iancowie/5018093/History-does-not-repeat-itself-but-it-often-rhymes-as-Mark-Twain-noted.html>

Cox, J. (2015). *The Dark Web as You Know It Is a Myth* | WIRED. Retrieved May 31, 2019, from <https://www.wired.com/2015/06/dark-web-know-myth/>

Cox, J. (2016). *7 Ways the Cops Will Bust You on the Dark Web*. Retrieved from https://motherboard.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web

Cox, J. (2016). Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets. *Insights*, 21, 49-54.

Cox, J. (2016). Staying in the shadows: the use of bitcoin and encryption in cryptomarkets. In *The Internet and drug markets* (pp. 41-47). Publications of the European Union.

Cox, R. W., Johnson, T. A., & Richards, G. E. (2009). Routine activity theory and Internet crime. *Crimes of the Internet*, 302-316.

Coyne, I., Farley, S., Axtell, C., Sprigg, C., Best, L., & Kwok, O. (2017). Understanding the Relationship Between Experiencing Workplace Cyberbullying, Employee Mental Strain and Job Satisfaction: A Dysempowerment Approach. *International Journal of Human Resource Management*, 28(7), 945-972. doi:10.1080/09585192.2015.1116454

Cranor, L. F. (2004). I didn't buy it for myself. In *Designing personalized user experiences in eCommerce* (pp. 57-73). Academic Press.

Compilation of References

- Cranor, L., Joseph, R., & Ackerman, M. (1999). Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. In Telecommunications Policy Research Conference (pp. 25-27). Academic Press.
- Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*, 12(3), 287–299. doi:10.1080/13552600601069414
- Creswell, J., & Poth, C. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, CA: SAGE Publications.
- Criado Grande. (2012). *Las redes sociales digitales en las administraciones públicas iberoamericanas: retos y perspectivas de futuro*. CLAD.
- Criddle, L. (2017). *What is Social Engineering? Examples and Prevention Tips*. Retrieved from <https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering>
- Crime and Misconduct Commission Queensland. (2013). *Fraud, financial management and accountability in the Queensland public sector - an examination of how a \$16.69 million fraud was committed on Queensland Health*. Author.
- Crime, E. T. O. C. (2011). Why Lawyers Need To Understand It. *Pittsburg Journal of Technology Law & Policy*, 11(4), 1-54. Retrieved November 3, 2018, from <https://tlp.law.pitt.edu/ojs/index.php/tlp/article/download/62/62>
- Cross, C. (2018). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In *The Palgrave handbook of criminology and the global south* (pp. 261–280). Springer. doi:10.1007/978-3-319-65021-0_14
- Crossen, S. (2015). *The Mathematics of Bitcoin* (Master Thesis). Department of Mathematics Emporia State University.
- Croteau, D., & Hoynes, W. (2013). *Experience sociology*. New York: McGraw-Hill Companies Inc.
- Crozier, R. (2019, February 14). *Aussie IT firms cop customer trust hit as encryption laws bite*. Retrieved from <https://www.itnews.com.au/news/aussie-it-firms-cop-customer-trust-hit-as-encryption-laws-bite-519286>
- Cruz, P. D., & Noronha, E. (2017). Workplace cyberbullying : Insights into an emergent phenomenon. In K. Chillas, Briken, M. Krzywdzinski, & A. Marks (Eds.), *The new digital workplace: How new technologies revolutionise work* (pp. 112–131). London: Palgrave.
- CSO. (2018). *9 cyber security predictions: Our hopes (and fears) for the infosec world for the coming year*. CSO, IDG Communications, Inc. Retrieved from <https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html>
- Cubrilovic, N. (2014). *Large number of tor hidden sites seized by the fbi in operation anonymous were clone or scam sites*. Retrieved from <https://www.nikcub.com/posts/onymous-part1>
- Culnan, M. J., McHugh, P. J., & Zubillaga, J. I. (2010). How Large U.S. Companies Can Use Twitter and Other Social Media to Gain Business Value. *MIS Quarterly Executive*, 9(4), 243–259.
- Curelaru, M., Iacob, I., & Abalasei, B. (2009). *School bullying: Definition, characteristics, and intervention strategies*. Lumean Publishing House.
- Curran, B. (2018). *How Formal Verification Can Reduce Bugs & Vulnerabilities in Smart Contracts*. Retrieved from <https://blockonomi.com/formal-verification-smart-contracts/>
- Curtin Singapore's website defaced by hackers claiming to represent ISIS. (2015, March 10). *Today*. Retrieved from <https://www.todayonline.com/singapore/curtin-singapores-website-defaced-hackers-claiming-represent-isis>

Curtom, G. (2014, April 24). Students punished for expressing free speech on Twitter. The Cougar. Retrieved from <http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/>

CWE List Version 3.1. (2017). Retrieved December 7, 2018, from <https://cwe.mitre.org/data/index.html>

Cyber Aware. (n.d.). Retrieved from <https://www.cyberaware.gov.uk>

Cyber Civil Rights Initiative. (n.d.). *40 states + DC now have revenge porn laws*. Retrieved from <https://www.cyber-civilrights.org/revenge-porn-laws/>

Cyber Security Campaign. (n.d.). Retrieved from <https://www.cybersecuritycampaign.com.hk/index-en.html#>

Cyberbullying Research Center. (2018). *Sexting Laws Across America*. Retrieved from <https://cyberbullying.org/sexting-laws>

Cybersecurity Ventures. (2017). *Cybercrime Report*. Retrieved September 29, 2018, from <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

Cybrary. (2016, October). *Cybercrime and the gaming industry*. Retrieved from <https://www.cybrary.it/2016/10/cybercrime-gaming-industry/>

D'Alessio, D., & Stolzenberg, L. (2002). A multilevel analysis of the relationship between labour surplus and pretrial incarceration. *Social Problems*, 49(2), 178–193. doi:10.1525p.2002.49.2.178

D'Angelo, W. (2018, March). PS4 vs Xbox One vs Switch global lifetime sales – January 2018 – sales. *VGChartz Ltd*. Retrieved from <http://www.vgchartz.com/article/272742/ps4-vs-xbox-one-vs-switch-global-lifetime-salesjanuary-2018/>

D'ecary-H'etu, D., Morselli, C., & Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among warez hackers. *Journal of Research in Crime and Delinquency*, 49(3), 359–382. doi:10.1177/0022427811420876

DaCosta, B., Seok, S., & Kinsell, C. (2015). Mobile games and learning. In Z. Yan (Ed.), *Encyclopedia of mobile phone behavior* (Vol. 1, pp. 46–60). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8239-9.ch004

Dagaci, Magaji, & Damagun. (2014). Cybercrimes and Victimization: An Analysis of Economic Cost Implications to Nigeria. In *Handbook on the Emerging Trends in Scientific Research*. ICETSR.

Daily Mail Reporter. (2011, April). We've been hacked: Sony finally blames 'external intrusion' for PlayStation network outage. *Daily Mail*. Retrieved from <https://www.dailymail.co.uk/sciencetech/article-1380050/Sony-admits-Weve-hacked-PlayStation-Network-outage.html>

Dalins, J., Wilson, C., & Carman, M. (2017). Criminal motivation on the dark web: A categorization model for law enforcement. *Digital Investigation*, 24, 62–71. doi:10.1016/j.diin.2017.12.003

Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation*, 24, 62–71. doi:10.1016/j.diin.2017.12.003

Dalvi, N., Kumar, R., Pang, B., Ramakrishnan, R., Tomkins, A., Bohannon, P., ... Merugu, S. (2009, June). A web of concepts. In *Proceedings of the twenty-eighth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (pp. 1-12). ACM.

Danermark, B., Ekström, M., Jakobsen, L., & Karlsson, J. C. (1997). Generalization, scientific inference and models for an explanatory social science. *Explaining Society: Critical Realism in the Social Sciences*, 73–114.

Dange, V. R., Malkan, K., & Jha, M. (2018). *Monograph on Dark Web*. Dhole Patil College of Engineering, Department of Computer Engineering. Pune: Pune: Dhole Patil College of Engineering.

Compilation of References

- Dank, M., Khan, B., Downey, P. M., Kotonias, C., Mayer, D., Owens, C., & Yu, L. (2014). Estimating the size and structure of the underground commercial sex economy in eight major US cities. *The Urban Institute*. Retrieved from <https://www.urban.org/sites/default/files/alfresco/publication-pdfs/413047Estimating-the-Size-and-Structure-of-the-Underground-Commercial-Sex-Economy-in-Eight-MajorUS-Cities.PDF>
- Dankar, F. K., & Al Ali, R. (2015). A theoretical multi-level privacy protection framework for biomedical data warehouses. *Procedia Computer Science*, 63, 569–574. doi:10.1016/j.procs.2015.08.386
- Danquah, P., & Longe, O. B. (2011). Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact*, 11(3), 169–182.
- Darczewska, J., & Żochowski, P. (2017). Active Measures: Russia's Key Export. *OSW Studies*, 64.
- Dascalescu, A. (2018, January 3). Doxxing Can Ruin Your life. Here's How (You Can Avoid It). Retrieved May 17, 2019, from Heimdal Security website: <https://heimdalsecurity.com/blog/doxxing/#doxxingswatting>
- Das, R. C., & Mukherjee, S. (2018). Determinants of Terrorism in South Asia: Insights From a Dynamic Panel Data Analysis. *International Journal of Cyber Warfare & Terrorism*, 8(4), 16–34. doi:10.4018/IJCWT.2018100102
- Davidson, J., & Gottschalk, P. (2011). Characteristics of the Internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies*, 24(1), 23–36. doi:10.1080/1478601X.2011.544188
- Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation). Massachusetts Institute of Technology.
- Davis, S., & Nixon, Cl. (2012). Empowering bystanders. In J. Patchin & S. Hinduja (Eds.), *Cyberbullying Prevention and Response: Expert Perspectives* (pp. 93–113). New York, NY: Routledge.
- Dawson, M., Omar, M., & Abramson, J. (n.d.). Understanding the Methods behind Cyber Terrorism. *Encyclopedia of Information Science and Technology, Third Edition*, 1539–1549. doi:10.4018/978-1-4666-5888-2.ch147
- Day, H. D., Franklyn, J. M., & Marshall, J. J. (1998). Predictions of aggression in hospitalized adolescents. *The Journal of Psychology*, 132(4), 427–435. doi:10.1080/00223989809599277 PMID:9637024
- De George, R. T. (1986). Whistleblowing. In *Business Ethics* (pp. 221–238). New York: Macmillan Publishing Company.
- De Wet, J. A., Labuschagne, G. N., & Chiroro, P. M. (2009). Offender Characteristics of the South African Male Serial Rapist: An Exploratory Study. *Acta Criminologica, Southern African Journal of Criminology*, 22(1), 37–45.
- Deakin University. (2017, October). *Video game cyber crime is a \$50 billion industry: Deakin expert*. Retrieved from [http://www.deakin.edu.au/about-deakin/media-releases/articles/video-game-cyber-crime-is-a-\\$50-billion-industry-deakin-expert](http://www.deakin.edu.au/about-deakin/media-releases/articles/video-game-cyber-crime-is-a-$50-billion-industry-deakin-expert)
- Dearden, L. (2019, August 25). Revered as a saint by online extremists, how Christchurch shooter inspired copycat terrorists around the world. *Independent*. Retrieved from <https://www.independent.co.uk/news/world/australasia/brenton-tarrant-christchurch-shooter-attack-el-paso-norway-poway-a9076926.html>
- Dearden, L. (2018). *Five British men have killed themselves after falling victim to online 'sextortion', police reveal*. Independent.
- Décary-Héty, D., Mousseau, V., & Vidal, S. (2018). Six Years Later: Analyzing Online Black Markets Involved in Herbal Cannabis Drug Dealing in the United States. *Contemporary Drug Problems*, 45(4), 366–381. doi:10.1177/0091450918797355

- DeHart, D., Dwyer, G., Seto, M. C., Moran, R., Letourneau, E., & Schwarz-Watts, D. (2016). Internet sexual solicitation of children: A proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression*, 23(1), 77–89. doi:10.1080/13552600.2016.1241309
- Dehue, F., Bolman, C., & Vollink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. *CyberPsychology & Behavior*, 11(2), 217–223. doi:10.1089/cpb.2007.0008 PMID:18422417
- Dehue, F., Bolman, C., Vollink, T., & Pouwelse, M. (2012). Cyberbullying and traditional bullying in relation to adolescents' perceptions of parenting. *Journal of Cyber Therapy and Rehabilitation*, 5, 25–34.
- deLara, E. W. (2012). Why adolescents don't disclose incidents of bullying and harassment. *Journal of School Violence*, 11(4), 288–305. doi:10.1080/15388220.2012.705931
- Deleuze, G., & Guattari, F. (2014). Post modernity as schizoid desire cited. In A. Elliot (Ed.), *Contemporary social theory: An introduction* (2nd ed.; pp. 254–258). New York: Routledge.
- Dell. (n.d.). Retrieved from Dell: https://www.dell.com/downloads/ca/support/top_10_steps_to_protect_against_cyber-crime_dell_en.pdf
- Dellaert, B. G. C., & Kahn, B. E. (1999). How tolerable is delay?: Consumers' evaluations of internet web sites after waiting. *Journal of Interactive Marketing*, 13(1), 41–54. doi:10.1002/(SICI)1520-6653(199924)13:1<41:AID-DIR4>3.0.CO;2-S
- Deloitte. (2016). *European union intellectual property office report: Research on online business models infringing intellectual property rights*. EUIPO.
- Deloitte. (2017). *Privacy is paramount: Personal data protection in Africa*. Retrieved October 12, 2018, https://www2.deloitte.com/.../za_Privacy_is_Paramount-Personal_Data_Protection_in_
- Deng, S., Liu, Y., & Qi, Y. (2011). An empirical study on determinants of web based question-answer services adoption. *RE:view*, 35(5), 789–798.
- Denning, D. (2015, September 8). The rise of hacktivism. *Georgetown Journal of International Affairs*. Retrieved from <https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism>
- Denning, D. E. (2012). Stuxnet: What Has Changed? *Future Internet*, 4(3), 672–687. doi:10.3390/fi4030672
- Denno, D. (1985). Sociology and human developmental explanations of crime: Conflict or Consensus? *Criminology*, 23(4), 141–174. doi:10.1111/j.1745-9125.1985.tb00371.x
- Department of Homeland Security. (2014). *What is human trafficking?* Retrieved from <http://www.dhs.gov/definition-human-trafficking>
- Department of Statistics Malaysia. (2018). *ICT Use and Access by Individuals and Households Survey Report, Malaysia, 2017*. Released March 19, 2018. Retrieved December 1, 2018 from https://www.dosm.gov.my/v1/index.php?r=column/cthemByCat&cat=395&bul_id=bHBZbWxkWEIxDlmaU81Q3R2ckRkZz09&menu_id=amVoWU54UTl0a21NWm dhMjFMMWcyZz09
- Deshpande, N. A., & Nour, N. M. (2013). Sex trafficking of women and girls. *Reviews in Obstetrics & Gynecology*, 6(1), e22–e27. PMID:23687554
- DeSot, T. (2017, January 13). *The Sorry State Of Cybersecurity Awareness Training*. Retrieved from Dark Reading: <https://www.darkreading.com/vulnerabilities---threats/the-sorry-state-of-cybersecurity-awareness-training/a/d-id/1327862>
- Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., & Hierons, R. (2018). *Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering?* IEEE.

Compilation of References

- Dewan, P., Kashyap, A., & Kumaraguru, P. (2014). Analyzing social and stylo metric features to identify spear phishing emails. *Electronic Crime Research (eCrime), 2014 APWG Symposium on, IEEE, 2014*, 1–13.
- DFC Intelligence. (2010, March). *Consumers & downloadable items*. Retrieved from <http://www.dfciint.com/dossier/consumers-downloadable-items/>
- Diamanduros, T., & Downs, E. (2011). Creating a safe school environment: How to prevent cyberbullying at your school. *Library Media Connection, 30*(2), 36–38.
- Diamond, J. (2017). *Flashback: Unabomber publishes his 'Manifesto'*. Retrieved from <https://www.rollingstone.com/culture/culture-news/flashback-unabomber-publishes-his-manifesto-125449/>
- Dickson, B. (2016, June). The gaming industry can become the next big target of cybercrime. *Crunch Network*. Retrieved from <https://techcrunch.com/2016/06/08/the-gaming-industry-can-become-the-next-big-target-of-cybercrime/>
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654. doi:10.1109/TIT.1976.1055638
- DiFonzo, N., Suls, J., Beckstead, J.W., Bourgeois, M.J., Homan, C.M., Brougher, S., Younge, A.J. & Terpstra-Schwab, N. (2014). Network Structure Moderates Intergroup Differentiation of Stereotyped Rumors. *Social Cognition, 32*(5), 409-448. doi:10.1521/oco.2014.32.5.409
- Digital Rights Ireland and Seitlinger. C-293/12 and C-594/12 (Court of Justice of the European Union April 8, 2014). Retrieved September 29, 2018, from <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
- Dillon, L. (2016). Cyberterrorism: Using the internet as a weapon of destruction. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 426–451). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch021
- Dindia, K. (2002). Self -disclosure research: Knowledge through meta-analysis. In M. Allen, R. W. Preiss, B. M. Gayle, & N. A. Burrell (Eds.), *LEA's Communication Series. Interpersonal communication research: Advances through meta-analysis* (pp. 169–185). Mahwah, NJ: Lawrence Erlbaum Associates.
- Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The Second-Generation Onion Router*. Retrieved from https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router
- Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics, 9*(4), 384–410. doi:10.1080/15027570.2010.536404
- DiResta, R. (2018). *Free Speech Is Not the Same As Free Reach*. Retrieved from <https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/>
- Dissecting a Hactivist Attack. (2012). *Computer Fraud & Security, (6)*, 3.
- Dix, E. L., Emery, L. F., & Le, B. (2014). Committed to the honor code: An investment model analysis of academic integrity. *Social Psychology of Education, 17*(1), 179–196. doi:10.1007/11218-013-9246-2
- Doan, A., Halevy, A., & Ives, Z. (2012). *Principles of data integration*. Elsevier.
- Doddington, G. R., Mitchell, A., Przybicki, M. A., Ramshaw, L. A., Strassel, S., & Weischedel, R. M. (2004, May). The Automatic Content Extraction (ACE) Program-Tasks, Data, and Evaluation. In LREC (Vol. 2, p. 1). Academic Press.
- Dolgun, U. (2005). *Enformasyon Toplumundan Gözetim Toplumuna*. Ankara: Ekin Kitabevi.

- Döllinger, D. (1984). Probleme der Aktenanalyse in der Kriminologie. In *Methodologische Probleme in der kriminologischen Forschungspraxis* (pp. 265–286). Heidelberg, Germany: Academic Press.
- Dolliver, D. S., Ericson, S. P., & Love, K. L. (2018). A Geographic Analysis of Drug Trafficking Patterns on the TOR Network. *Geogr Rev*, 108(1), 45–68. doi:10.1111/gere.12241
- Dolu, O. (2013). Suç ve Sapma Teorileri. In A. Geleri (Ed.), *Suç Sosyolojisi* (pp. 3–24). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.
- Domas, C. (2017). *Breaking the x86 ISA*. Black Hat.
- Domestic violence: Orders of protection and restraining orders. (2018). Retrieved from <https://family.findlaw.com/domestic-violence/domestic-violence-orders-of-protection-and-restraining-orders.html>
- Domingo-Ferrer, J., & Mateo-Sanz, J. M. (2002). Practical data-oriented microaggregation for statistical disclosure control. *IEEE Transactions on Knowledge and Data Engineering*, 14(1), 189–201. doi:10.1109/69.979982
- Domingos, P. (2018). *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. Basic Books.
- Dominioni, S. (2018, July 16). *Multilateral tracks to tackling cybercrime: an overview*. Retrieved November 5, 2018, from Italian Institute for International Political Studies: <https://www.ispionline.it/en/pubblicazione/multilateral-tracks-tackling-cybercrime-overview-20962>
- Domke, F. (2006). Console hacking 2006. *23rd Chaos Communication Congr.*
- Domke, F., & Steil, M. (2007). Why Silicon-Based Security is still hard: Deconstructing XBOX 360 Security. *24th Chaos Communication Congr.*
- Domke, F., Steil, M., & Reilink, R. (2004). Game cube hacking *21st Chaos Communication Congr.*
- Donegan, R. (2012). Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis. *The Elon Journal of Undergraduate Research in Communications*, 3(1), 33–42.
- Dong, X. L., & Srivastava, D. (2013, April). Big data integration. In *Data Engineering (ICDE), 2013 IEEE 29th International Conference on* (pp. 1245–1248). IEEE. 10.1109/ICDE.2013.6544914
- Dönmezer, S. (1999). *Toplumbilim*. İstanbul: Beta Yayınları.
- Dooley, J. J., Pyzalski, J., & Cross, D. (2009). Cyberbullying Versus Face-to-Face Bullying A Theoretical and Conceptual Review. *The Journal of Psychology*, 217(4), 182–188. doi:10.1027/0044-3409.217.4.182
- Dornfeld, L., & Mezei, K. (2017). Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog*, 14(68), 32–37.
- Dornfeld, L. (2016). A kiberbűncselekmények nyomozásával kapcsolatban folytatott uniós bűnügyi együttműködés fejlődése. *Külgügyi Szemle*, 15(4), 89–101.
- Dorn, W. (2017). *Cyberpeacekeeping: A New Role for the United Nations?* (Vol. 18). Georgetown Journal of International Affairs.
- Downward, P., & Mearman, A. (2006). Retrodution as mixed-methods triangulation in economic research: Reorienting economics into social science. *Cambridge Journal of Economics*, 31(1), 77–99. doi:10.1093/cje/bel009

Compilation of References

- Doyle, S. (2011). But How Do You Know it's Sexist? The #MenCallMeThings Round-Up. *Tiger Beatdown*. Retrieved 10th of October 2018 from <http://www.tigerbeatdown.com/2011/11/10/but-how-do-you-know-its-sexist-the-mencall-methings-round-up/>
- Drazen, P. (2014). *Anime Explosion!: The What? Why? and Wow! of Japanese Animation*. Stone Bridge Press.
- Dressing, H., & Foerster, K. (2010). Erotomanie, pathologische Verliebtheit, kognitive Distorsionen: Psychopathologische Übergänge beim Stalking. *Forensische Psychiatrie, Psychologie, Kriminologie*, 4(3), 155–159. doi:10.1007/11757-010-0058-3
- Dressing, H., Kühner, C., & Gass, P. (2005). Lifetime prevalence and impact of stalking in a European population: Epidemiological data from a middle-sized German City. *The British Journal of Psychiatry*, 187(AUG), 168–172. doi:10.1192/bjp.187.2.168 PMID:16055829
- Dressing, H., Kühner, C., & Gass, P. (2007). Multiaxiale Klassifikation von Stalkingfällen. *Der Nervenarzt*, 78(7), 764–772. doi:10.1007/00115-006-2205-9 PMID:17119890
- Drozdiak, N. (2018, September 26). Google, Facebook and Twitter Agree to Fight Fake News in the EU. *Bloomberg*. Retrieved from <https://www.bloomberg.com/news/articles/2018-09-25/google-facebook-and-twitter-agree-to-fight-fake-news-in-eu>
- Drug Trafficking. (2017). *New World Encyclopedia*. Retrieved from http://www.newworldencyclopedia.org/entry/Drug_trafficking
- Drzik, J. (2018, January 17). Cyber risk is a growing challenge. So how can we prepare? *World Economic Forum*. Retrieved from <https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready>
- Dubraski, A., Miller, K., Barnes, M., Boecking, B., & Kennedy, E. (2015). Leveraging publicly available data to discern patterns of human-trafficking activity. *Journal of Human Trafficking*, 1(1), 65–85. doi:10.1080/23322705.2015.1015342
- Duckworth, N., & de Silva, E. (2016). In I. G. I. Global (Ed.), *Teaching new dogs old tricks: The basics of espionage transcend time. In National Security and Counterintelligence in the Era of Cyber Espionage* (pp. 76–95). doi:10.4018/978-1-4666-9661-7.ch005
- Duff, A. (2008). The Normative Crisis of the Information Society. *Cyberpsychology (Brno)*, 2(1). Retrieved from <http://cyberpsychology.eu/view.php?cisloclanku=2008051201&article=3>
- Duffy, J. (1975). IFToMM symposium—Dublin, September 1974. *Mechanism and Machine Theory*, 10(2-3), 269. doi:10.1016/0094-114X(75)90030-0
- Duffy, M. (2009). Preventing Workplace Mobbing and Bullying with Effective Organizational Consultation, Policies, and Legislation. *Consulting Psychology Journal: Practice and Research*, 61(3), 242–262. doi:10.1037/a0016578
- Duggan, M. (2017). *Online harassment 2017*. Retrieved 10th of October 2018 from <http://www.pewinternet.org/2017/07/11/online-harassment-2017/>
- Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. (2013). *Fundamentals of Business Process Management*. Springer. doi:10.1007/978-3-642-33143-5
- Dungan, J., Waytz, A., & Young, L. (2015). The psychology of whistleblowing. *Current Opinion in Psychology*, 6, 129–133. doi:10.1016/j.copsyc.2015.07.005

- Dunn, A. (2018). *Trump's Approval Ratings So Far Are Unusually Stable - And Deeply Partisan*. Pew Research Center. Retrieved from <http://www.pewresearch.org/fact-tank/2018/08/01/trumps-approval-ratings-so-far-are-unusually-stable-and-deeply-partisan/>
- DuPont, Q. (2017). *Experiments in Algorithmic Governance*. Retrieved from <https://web.archive.org/web/20170730133911/http://iqdupont.com/assets/documents/DUPONT-2017-Preprint-Algorithmic-Governance.pdf>
- Durkee, A. (2019, June 5). YouTube is finally taking a harder line on hate speech. Is it too little, too late? *Hive*. Retrieved from <https://www.vanityfair.com/news/2019/06/youtube-hate-speech-too-little-too-late>
- Durkee, M. J. (2017). Astroturf Activism. *Stanford Law Review*, 69(1), 201-268. Retrieved from <https://review.law.stanford.edu/wp-content/uploads/sites/3/2017/01/69-Stan-L-Rev-201.pdf>
- Durkin, K. F., & Brinkman, R. (2009). 419 FRAUD: A crime without borders in A postmodern world. *International Review of Modern Sociology*, 271-283.
- Dvorsky, G. (2017, September 11). *Hackers Have Already Started to Weaponize Artificial Intelligence*. Gizmodo.
- Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81-91. doi:10.1016/j.jfs.2014.11.006
- Dyer, K. (2010). Challenges of maintaining academic integrity in an age of collaboration, sharing, and social networking. In *Proceedings of TCC 2010* (pp. 168-195). Academic Press.
- Dyer, T. (2018). *Hactivist or cyberterrorist? Understanding the difference between hacktivism and cyber terrorism* (Doctoral dissertation). ProQuest Dissertations and Theses.
- Dyer, O. (2005). Consultants who misled Shipman inquiry are found guilty of misconduct. *BMJ : British Medical Journal*, 331(7524), 1042. doi:10.1136/bmj.331.7524.1042-d PMID:16269475
- Dziembowski, S. (2015). Introduction to Cryptocurrencies. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15* (pp. 1700-1701). New York: ACM Press. 10.1145/2810103.2812704
- Eastin, M., Greenberg, B., & Hofschire, L. (2006). Parenting the Internet. *Journal of Communication*, 56(3), 486-504. doi:10.1111/j.1460-2466.2006.00297.x
- Easton, G. (2010). Critical realism in case study research. *Industrial Marketing Management*, 39(1), 118-128. doi:10.1016/j.indmarman.2008.06.004
- Eastwood, G. (2017). *5 of the biggest cybersecurity risks surrounding IoT development*. Retrieved 2018, September 17, from <https://www.networkworld.com/article/3204007/internet-of-things/5-of-the-biggest-cybersecurity-risks-surrounding-iot-development.html>
- Eaton, A. A., Jacobs, H., & Ruvalcaba, Y. (2017). *2017 Nationwide online study of nonconsensual porn victimization and perpetration: A summary report*. Cyber Civil Rights Initiative. Retrieved from <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>
- Echevarria, A. I. (2016). *Operating in the gray zone: An alternative paradigm for US military strategy*. Army War College-Strategic Studies Institute Carlisle United States.
- Eckersley, P. (2010). *How unique is your web browser? Privacy Enhancing Technologies*. Springer.
- Ecker, U. K., Lewandowsky, S., Fenton, O., & Martin, K. (2014). Do people keep believing because they want to? Preexisting attitudes and the continued influence of misinformation. *Memory & Cognition*, 42(2), 292-304. doi:10.375813421-013-0358-x PMID:24005789

Compilation of References

- Eck, J. E., & Clarke, R. V. (2003). Classifying Common Police Problems: A Routine Activity Approach. *Crime Prevention Studies*, 16, 7–39.
- Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies*, 16, 7–40.
- Economist. (2017). *Buying drugs online, Shedding light on the dark web*. Retrieved from <https://www.economist.com/international/2016/07/16/shedding-light-on-the-dark-webon>
- ECPAT International. (2013, August 27). *Today is the Anniversary of the First World Congress against the Commercial Sexual Exploitation of Children*. Retrieved from <http://www.ecpat.org/news/today-anniversary-first-world-congress-against-commercial-sexual-exploitation-children/>
- Edelman, B. (2015). Retrieved from Affiliate fraud litigation index: [http:// www.benedelman.org/affiliate-litigation](http://www.benedelman.org/affiliate-litigation)
- Edelman, B., & Brandi, W. (2015, February). Risk, Information, and Incentives in Online Affiliate Marketing. *JMR, Journal of Marketing Research*, 52(1), 1–12. doi:10.1509/jmr.13.0472
- Edelman, M. (1985). Political language and political reality. *PS, Political Science & Politics*, 18(1), 10–19. doi:10.1017/S1049096500021247
- Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H., . . . (2016). Forensic readiness for SCADA/ICS incident response. In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research* (pp. 1-9). Swindon, UK: BCS Learning & Development Ltd. 10.14236/ewic/ICS2016.16
- Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., & Soulsby, H. (2016). A Cyber Forensic Taxonomy for SCADA Systems in Critical Infrastructure. In E. Rome, M. Theocharidou, & S. Wolthusen (Eds.), *Lecture Notes in Computer Science: Vol. 9578. Critical Information Infrastructures Security. CRITIS 2015* (pp. 27–39). Springer. doi:10.1007/978-3-319-33331-1_3
- Eden, S., Heiman, T., & Olenik-Shemesh, D. (2013). Teachers' perceptions, beliefs and concerns about cyberbullying. *British Journal of Educational Technology*, 44(6), 1036–1052. doi:10.1111/j.1467-8535.2012.01363.x
- Edwards, K. (2009). Commencing unemployment. *Economic Policy Institute*. Available at <http://epi.org>
- Edwards, C., & Gribbon, L. (2013). Pathways to violent extremism in the digital era. *The RUSI Journal*, 158(5), 40–47. doi:10.1080/03071847.2013.847714
- Egger, C., Schlumberger, J., Kruegel, C., & Vigna, G. (2013). Practical attacks against the i2p network. In *International workshop on recent advances in intrusion detection* (pp. 432–451). Academic Press.
- Eggers, D. (2013). *The Circle*. McSweeney's Books.
- Eichensehr, K. E. (2017). Data Extraterritoriality. *Texas Law Review*, 95, 145–160.
- Einav, L., & Levin, J. (2014). The data revolution and economic analysis. *National Bureau of Economic Research*, 14, 1-24. Retrieved from <https://www.nber.org/chapters/c12942.pdf>
- Eirinaki, M., Gao, J., Varlamis, I., & Tserpes, K. (2018). Recommender systems for large-scale social networks: A review of challenges and solutions. *Future Generation Computer Systems*, 78, 413–418. doi:10.1016/j.future.2017.09.015
- Eklblom, P. (2014). Designing products against crime. In *Encyclopedia of Criminology and Criminal Justice* (pp. 948–957). Springer. doi:10.1007/978-1-4614-5690-2_551

- El Emam, K., & Arbuckle, L. (2013). *Anonymizing health data: case studies and methods to get you started*. O'Reilly Media, Inc.
- El Emam, K., Rodgers, S., & Malin, B. (2015). Anonymising and sharing individual patient data. *BMJ (Clinical Research Ed.)*, 350(1), h1139. doi:10.1136/bmj.h1139 PMID:25794882
- Elangovan, R., & Prianga, M. (2019). Side Channel Attacks in Cloud Computing. In *Cognitive Social Mining Applications in Data Analytics and Forensics* (pp. 77-98). IGI Global. doi:10.4018/978-1-5225-7522-1.ch005
- ElEconomista.com. (2019). *Facebook CL A*. Available at <http://www.eleconomista.es/empresa/FACEBOOK>
- Elledge, L. C., Williford, A., Boulton, A. J., DePaolis, K. J., Little, T. D., & Salmivalli, C. (2013). Individual and contextual predictors of cyberbullying: The influence of children's provictim attitudes and teachers' ability to intervene. *Journal of Youth and Adolescence*, 42(5), 698–710. doi:10.1007/10964-013-9920-x PMID:23371005
- Elmagarmid, A. K., Ipeirotis, P. G., & Verykios, V. S. (2007). Duplicate record detection: A survey. *IEEE Transactions on Knowledge and Data Engineering*, 19(1), 1–16. doi:10.1109/TKDE.2007.250581
- El-Masri, R., & Wiederhold, G. (1979, May). Data model integration using the structural model. In *Proceedings of the 1979 ACM SIGMOD international conference on Management of data* (pp. 191-202). ACM. 10.1145/582095.582127
- Elwell, C. K., Murphy, M. M., & Seitzinger, M. V. (2013). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Academic Press.
- Emam, K. El. (2013). *Guide to the De-Identification of Personal Health Information*. doi:10.1201/b14764
- Emarketer.com. (2014). Worldwide Ecommerce Sales to Increase Nearly 20% in 2014 - eMarketer. Retrieved November 22, 2017, from <https://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039>
- Emerging Trends In Global Cyber Crime. (2017). Retrieved from Maryville University: <https://online.maryville.edu/blog/emerging-trends-in-global-cyber-crime/>
- Englehardt, S., & Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery. 10.1145/2976749.2978313
- Ennew, C., & Sekhon, H. (2007). Measuring trust in financial services: The trust index. *Consumer Policy Review*, 17(2), 62–68.
- Epler, P. (2013). Using the Response to Intervention (RtI) Service Delivery Model in Middle and High Schools. *International Journal for Cross-Disciplinary Subjects in Education*, 4(1), 1089–1098. doi:10.20533/ijcdse.2042.6364.2013.0154
- Erdur-Baker, O. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools. *New Media & Society*, 12(1), 109–125. doi:10.1177/1461444809341260
- Ericsson ConsumerLab. (2014) Retrieved October, 11 2018, from, <http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf>
- Ermakova, T., Fabian, B., Baumann, A., Izmailov, M., & Krasnova, H. (2017). *Bitcoin: Drivers and Impediments*. Available at SSRN 3017190
- Ernst, P., Siu, A., Milchevski, D., Hoffart, J., & Weikum, G. (2016). Deeplife: An entity-aware search, analytics and exploration platform for health and life sciences. *Proceedings of ACL-2016 System Demonstrations*, 19-24. 10.18653/v1/P16-4004

Compilation of References

- ESA. (2018). 2018 sales, demographic, and usage data. Essential facts about the computer and video game industry. *Entertainment Software Association*. Retrieved from http://www.theesa.com/wp-content/uploads/2018/05/EF2018_FINAL.pdf
- Etzioni, O., Banko, M., Soderland, S., & Weld, D. S. (2008). Open information extraction from the web. *Communications of the ACM*, 51(12), 68–74. doi:10.1145/1409360.1409378
- European Commission Directorate-General Migration And Home Affairs. (n.d.). *Meeting report from the Internet and Drugs expert meeting*. Retrieved from https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/meeting_report_published.pdf
- European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open*. Brussels: Safe and Secure Cyberspace.
- European Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature Nov. 4, 1950, 213 UNTS 221, art. 10, (entered into force Sept. 3, 1953).
- European Institute for Gender Equality. (2017). *Cyber violence is a growing threat, especially for women and girls*. Retrieved from <https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls>
- European Parliament. (2018). *Cyber Violence and hate speech online against women Study for the FEMM Committee*. Retrieved 12th of November 2018 from [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU\(2018\)604979_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf)
- European Union. (2005, February 24). *Council Framework Decision 2005/222/JHA*. Retrieved from EUR-LEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN>
- European Union. (2016, May 4). (EU) 2016/679. *The protection of natural persons with regard to the processing of personal data and on the free movement of such data*. Retrieved November 25, 2018, from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
- European Women's Lobby. (2017) *#HerNetHerRights Resource Pack on ending online violence against women & girls in Europe*. Retrieved 12th of November 2018 from https://www.womenlobby.org/IMG/pdf/hernetherights_resource_pack_2017_web_version.pdf
- Europol, Drugs, and the Darknet. (2017). *Perspectives for enforcement, research and policy*. EMCDDA, Europol.
- Europol, E. P. O. (2018). *Take Control of Your Digital Life. Don't be a Victim of Cyberscams!* Retrieved December 4, 2018, from <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don-t-be-victim-of-cyber-scams>
- Europol. (2013). *Press Release: Global Action Against Dark Markets On Tor Network*. Retrieved from: <https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-networkon>
- Europol. (2014). *TE-SAT 2014. European Union terrorism situation and trend report 2014*. European Law Enforcement Agency.
- Europol. (2018). *Child sexual exploitation*. Retrieved from: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>
- Europol. (2018). *Internet Organised Crime Threat Assessment (IOCTA) 2018*. Retrieved December 7, 2018, from https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf
- Euzenat, J., & Shvaiko, P. (2013). Ontology Matching: State of the Art and Future Challenges. *IEEE Transactions on Knowledge and Data Engineering*, 25(1), 158–176. doi:10.1109/TKDE.2011.253

- Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. (2015). *International Journal of Drug Policy*, 26(11), 1113–1123. doi:10.1016/j.drugpo.2015.01.008
- Evans, C., Palmer, C., & Sleevi, R. (2015, April). *Public Key Pinning Extension for HTTP*. IETF. doi:10.17487/RFC7469
- evofit. (2018, 12 11). *Evolving Facial Composite Imaging*. Retrieved from <https://evofit.co.uk/>
- Evolutionary models of human drug use Wiki. (n.d.). Retrieved on 1st December, 2018, from https://en.wikipedia.org/wiki/Evolutionary_models_of_human_drug_use
- Executive Order 13800 (“Strengthening Cybersecurity of Federal Networks and Critical Infrastructure”) (2017, Jul 12). *Federal Register*, 82, 32172–32174.
- Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., & Song, D. (2018). *Robust Physical-World Attacks on Deep Learning Models*. *Computer Vision and Pattern Recognition*.
- Ezea, F. (2017). *An overview of Internet Governance and Infrastructure in the Philippines*. Foundation for Media Alternatives.
- Eze, B., & Peyton, L. (2015). Systematic Literature Review on the Anonymization of High Dimensional Streaming Datasets for Health Data Sharing. *Procedia Computer Science*, 63, 348–355. doi:10.1016/j.procs.2015.08.353
- Facebook - Security Centre. (n.d.). *Safety Bullying*. Retrieved December 10, 2018, from [Facebook.org](https://www.facebook.org)
- Facebook. (2018). *Connect with friends and the world around you on Facebook*. Retrieved from <https://www.facebook.com/>
- Facebook. (2018). *Facebook Newsroom - Company Info*. Retrieved from <https://newsroom.fb.com/company-info/>
- Fagan, J. A., & Pabon, E. (1990). Contributions of delinquency and substance use to school dropout. *Youth & Society*, 21(3), 306–354. doi:10.1177/0044118X90021003003
- Fairburn, C. G., & Patel, V. (2016). The impact of digital technology on psychological treatments and their dissemination. *Behaviour Research and Therapy*, 88, 19–25. doi:10.1016/j.brat.2016.08.012 PMID:28110672
- Falliere, N., Murchu, L. O., & Chien, E. (2011). *Stuxnet Dossier*. Symantec Security Response.
- Fallows, J. (2011, March 24). Cyber-security can’t ignore human behaviour. *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2011/03/cyber-security-cant-ignore-human-behavior/72826/>
- Fanti, K. A., Demetriou, A. G., & Hawa, V. V. (2012). A longitudinal study of cyberbullying: Examining risk and protective factors. *European Journal of Developmental Psychology*, 8(2), 168–181. doi:10.1080/17405629.2011.643169
- Faou, M., Lemay, A., Deary-Hetu, D., Calvet, J., Labreche, F., Jean, M., ... Fernandez, J. M. (2016). Follow the traffic: Stopping click fraud by disrupting the value chain. In *14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE. 10.1109/PST.2016.7907001
- Farina, J. (2000). *Defensa del consumidor y del usuario*. Buenos Aires: Ed. Astrea.
- Farivar, C. (2018, August 20). Man sues over Google’s “location history” fiasco, case could affect millions. *Ars Technica*. Retrieved from <https://arstechnica.com/tech-policy/2018/08/did-google-violate-users-privacy-when-it-secretly-kept-location-data/>
- Farley, S., Coyne, I., Axtell, C., & Subramanian, G. (2015). Exploring the Impact of Cyberbullying on Trainee Doctors. *Medical Education*, 49(4), 436–443. doi:10.1111/medu.12666 PMID:25800304

Compilation of References

- Farrell, P. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>
- Farrington, D. P. (2007). Human development and criminal career. In M. E. Vogel (Ed.), *Crime, inequality and the state*. New York: Routledge.
- Farrington, D. P. (1989). Early predictors of adolescent aggression and adult violence. *Violence and Victims*, 4(2), 79–100. doi:10.1891/0886-6708.4.2.79 PMID:2487131
- Farrington, D. P. (1992). Explaining the beginning, progress and ending of anti-social behaviour from birth to adulthood. In J. McCord (Ed.), *Facts, Frameworks and Forecasts: Advances in criminological theories*. New Brunswick, NJ: Transaction.
- Farrington, D. P. (1996). *Understanding and Preventing Youth Crime*. York, UK: Joseph Rowntree Foundation.
- Farwell, J. P. (2018). Countering Russian Meddling in US Political Processes. *Parameters*, 48(1), 37–47. Retrieved from https://ssi.armywarcollege.edu/pubs/Parameters/issues/Spring_2018/7_Farwell_CounteringRussianMeddling.pdf
- Fascendini, F., & Fialová, K. (2011). *Voices from digital spaces: Technology related violence against women*. Association for Progressive Communications. Retrieved 12th of November 2018 from https://www.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0_0.pdf
- FATF. (2014). *Virtual Currencies: Key Definations and potential AML/CFT Risks*. Geneva: Geneva Internet Platform. Retrieved from www.fatf-gafi.org
- Fati, M. (2016, August 23). *New artificial intelligence technology only delivers ads that actually change consumer opinion*. Retrieved from UK Tech News: https://www.uktech.news/press_release/new-artificial-intelligence-technology-delivers-ads-actually-change-consumer-opinion
- FBI. (2018). 2017 Internet Crime Report. Retrieved from https://pdf.ic3.gov/2017_ic3report.pdf
- Feathers, T. (2018, November 3). Deepfakes: the next threat to our elections? *New Hampshire Union Leader*. Retrieved from http://www.unionleader.com/news/politics/deepfakes-the-next-threat-to-our-elections/article_048c1795-7e51-51ad-8ce2-8b8121eedf15.html
- Federal Trade Commission. (1998). *Privacy Online: A Report to Congress*. Retrieved March 3, 2018 from available in <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>
- Federal Trade Commission. (2009). *The Can-SPAM Act: A Compliance Guide for Business*. Retrieved September 25, 2018 from <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>
- Felt, A., & Evans, D. (2009). Privacy protection for social networking APIs. *Proceedings of the Web 2.0 Security and Privacy W2SP 2009*.
- Ferasweelz. (2012, January 21). *How to cheat on an exam/test (it really works!)* [Video file]. Retrieved from <https://www.youtube.com/watch?v=g1I-7mHKitI>
- Fernandez Delpech, H. (2012). *Manual de Derecho Informático* (A. Perrot, Ed.). Buenos Aires: Academic Press.
- Fernandez, R. (2019). *Países con más usuarios de Facebook a nivel mundial 2019*. Available at <https://es.statista.com/estadisticas/518638/ranking-de-los-20-paises-con-mas-usuarios-de-facebook-a-nivel-mundial/>
- Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in social engineering and their use in phishing: Human aspects of information security, privacy, and trust. *Proceedings of the Third International Conference (HAS 2015)*.

- Ferreira, A., Machado, A., Costa, F. A., & Rezende, J. L. (2015). Use of simulation to achieve better results in cyber military training. *IEEE Military Communications Conference*.
- Ferrera, G. R. (2004). *Cyberlaw: text and cases* (2nd ed.). Mason, OH: Thomson/South-Western/West.
- Festl, R., Schwarkow, M., & Quandt, T. (2013). Peer influence, internet use and cyberbullying: A comparison of different context effects among German adolescents. *Journal of Children and Media*, 7(4), 446–462. doi:10.1080/17482798.2013.781514
- Fielding, N. G. (2017). The shaping of covert social networks: Isolating the effects of secrecy. *Trends in Organized Crime*, 20(1-2), 16–30. doi:10.1007/12117-016-9277-0
- Finch, E. (2003). What a tangled web we weave: Identity theft and the Internet. In Y. Jewkes (Ed.), *Dot.cons: Crime, deviance, and identity on the Internet* (pp. 86–104). Collompton, UK: Willan.
- FindLaw. (2018). *Nevada Prostitution and Solicitation Laws*. Retrieved from <https://statelaws.findlaw.com/nevada-law/nevada-prostitution-and-solicitation-laws.html>
- Finkelhor, D., & Araj, S. (1986). Explanations of pedophilia: A four-factor model. *Journal of Sex Research*, 22(2), 145–161. doi:10.1080/00224498609551297
- Finklea, K. (2017). *Dark Web*. Congressional Research Service. Retrieved from <https://fas.org/sgp/crs/misc/R44101.pdf>
- Firefox. (2019). *Mozilla Firefox*. Retrieved from <https://www.mozilla.org/en-US/firefox/new/>
- Fish, J. M., Reddish, C. J., & McCraw, S. J. (2004). *Fighting in the gray zone: a strategy to close the preemption gap*. DIANE Publishing.
- Fletcher, J. J., Sorrell, J. M., & Silvia, M. C. (1998). Whistleblowing as a failure of organizational ethics. *Online Journal of Issues in Nursing*, 3. Retrieved from <http://ojin.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Vol31998/No3Dec1998/Whistleblowing.aspx>
- Fletcher, J. J., Sorrell, M., & Silva, M. C. (1998). Whistleblowing as a failure of organizational ethics. *Online Journal of Issues in Nursing*, 3(3), 1–15.
- Flickr. (2018). *Flickr at its best is a place to connect, to discover, and to evolve as photographers and lovers of photography*. Retrieved from <https://www.flickr.com/>
- Flood-Page, C., Campbell, S., Harrington, V., & Miller, J. (2000). *Youth Crime: Findings from the 1998/99 Youth Life-styles Survey. Home Office Research Study 209*. London: Home Office.
- Foggeti, N. (2009). *Transnational Cybercrime Differences between national laws and development of European Legislation: By Repression?* Academic Press.
- Foo, S., & Jayakumar, S. (2018, January 26). Cyber threats: 2018 and beyond. *The Straits Times: Opinion*. Retrieved from <https://www.straitstimes.com/opinion/cyber-threats-2018-and-beyond>
- Foo, Y. C. (2018, September 26). Facebook, Google to tackle spread of fake news, advisors want more. *Reuters*. Retrieved from <https://www.reuters.com/article/us-eu-tech-fakenews/facebook-google-agree-to-tackle-fake-news-eu-idUSKCN1M61AG>
- Foody, M., Samara, M., & Carlbring, P. (2015). A review of cyberbullying and suggestions for online psychological therapy. *Internet Interventions*, 2(3), 235–242. doi:10.1016/j.invent.2015.05.002

Compilation of References

- Forbes. (2017). *The True Cost Of Cybercrime For Businesses*. Retrieved July 13, 2017, from Forbes website: <https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#16c370584947>
- Ford, M. (2018). *Architects of Intelligence: The truth about AI from the people building it*. Packt Publishing.
- Ford, R. A. (2005). Preemption of state spam laws by the federal CAN-SPAM Act. *The University of Chicago Review*, 72(1), 355–384.
- Forest, J. J. (2009). *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas*. ABC-CLIO.
- Forgo, N. (2010). Juristische Untersuchung. In *Forschungsbericht – Cyberstalking – Österreichweite Studie zum Cyberstalking-Verhalten* (p. 155). Wien: Huber.
- Formoso, J. (2017). *Human trafficking on the dark web and beyond*. Retrieved from <http://www.fox5ny.com/news/human-trafficking-on-the-dark-web-and-beyond>
- Forsen, G., Nelson, M., & Staron, R., Jr. (1977). *Personal attributes authentication techniques*. Technical Report RADCTR-77-333. Rome Air Development Center.
- Forssell, R. (2016). Exploring cyberbullying and face-to-face bullying in working life – prevalence, targets and expressions. *Computers in Human Behavior*, 58, 454–460. doi:10.1016/j.chb.2016.01.003
- Forster, P. (2005). *Queensland health system review – final report*. Brisbane: Queensland Parliament. Retrieved from <https://www.parliament.qld.gov.au/documents/tableOffice/TabledPapers/2005/5105T4447.pdf>
- Forsyth, J. W. Jr, & Pope, B. E. (2014). Structural causes and cyber effects: Why international order is inevitable in cyberspace. *Strategic Studies Quarterly*, 8(4), 112–128.
- Foucault, M. (2015). *Deliliğin Tarihi*. İstanbul: İmge Kitabevi.
- Fowler, F. C. (2013). *Policy studies for educational leaders: An introduction*. Boston, MA: Pearson.
- Franco, I. G. (2006). *Striving For Legality*. Retrieved, September, 20, 2018 from <http://www.ipfront.com/depts/articles.asp?id=13202&deptid=6>
- Frank, J. R., Kleiman-Weiner, M., Roberts, D. A., Niu, F., Zhang, C., Ré, C., & Soboroff, I. (2012). *Building an entity-centric stream filtering test collection for TREC 2012*. Massachusetts Inst of Tech.
- Freberg, K. (2012). Intention to Comply with Crisis Messages Communicated Via Social Media. *Public Relations Review*, 38(3), 416–421. doi:10.1016/j.pubrev.2012.01.008
- Freiling, F. C., Holz, T., & Wicherski, G. (2005) Botnet tracking: Exploring a root-cause methodology to prevent distributeddenial-of-service attacks. *Lecture Notes in Computer Science*, 3679, 319–335.
- Freitas, A., Curry, E., Oliveira, J. G., & O’Riain, S. (2012). Querying heterogeneous datasets on the linked data web: Challenges, approaches, and trends. *IEEE Internet Computing*, 16(1), 24–33. doi:10.1109/MIC.2011.141
- Frempong, G. (2012). *Understanding what is Happening in ICT in Ghana: A Supply-and Demand-side Analysis of the ICT Sector*. Academic Press.
- Frenkel, S. (2018, August 15). Real Posts from a Sham on Facebook. *New York Times*, p. B1.
- Frichot, C., Orru, M., & Alcorn, W. (2014). *The Browser Hacker’s Handbook*. Hoboken, NJ: Wiley.
- Froomkin, A.M. (1996). The internet as a source of regulatory arbitrage. *Asian Examples of Practical Limits to Censorship*.

- FTC.gov. (2017, September). The Equifax data breach: What to do. *Federal Trade Commission. Consumer Information*. Retrieved from <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>
- Furaker, B. (2009). Unemployment and social protection. In M. Guigni (Ed.), *Unemployment in Europe: Policy responses and policy action* (pp. 17–34). Padstow: TJ International Limited.
- Furman, W., & Buhrmester, D. (1992). Age and sex differences in perceptions of networks of personal relationships. *Child Development*, 63(1), 103–115. doi:10.2307/1130905 PMID:1551320
- Furnell, S. (2003). Cybercrime: Vandalizing the Information Society. In *Lecture Notes in Computer Science: Vol. 2722. International Conference on Web Engineering* (pp. 8-16). Berlin: Springer.
- Furnell, S. (2001). The Problem of Categorising Cybercrime and Cybercriminals. *Second Australian Information Warfare and Security Conference 2001*.
- Furnell, S. (2008). End user security culture - a lesson that will never be learnt? *Computer Fraud & Security*, 4, 6–9.
- Furnell, S., & Thompson, K. L. (2009). Recognising and addressing ‘security fatigue.’. *Computer Fraud & Security*, 11(11), 7–11. doi:10.1016/S1361-3723(09)70139-3
- Fussell, S. (2018, March 5). Moviepass CEO brags app tracks your location before and after movies. *Gizmodo*. Retrieved from <https://gizmodo.com/moviepass-ceo-brags-app-tracks-your-location-before-and-1823525088>
- Gabrilovich, E., & Markovitch, S. (2007, January). Computing semantic relatedness using wikipedia-based explicit semantic analysis. *IJCAI (United States)*, 7, 1606–1611.
- Gallidabino, M. D., Barron, L. P., Weyermann, C., & Romolo, F. S. (2018). Quantitative profile–profile relationship (QPPR) modelling: A novel machine learning approach to predict and associate chemical characteristics of unspent ammunition from gunshot residue (GSR). *Analyst (London)*. doi:10.1039/c8an01841c
- Gamallo, P., & Garcia, M. (2015, September). Multilingual open information extraction. In *Portuguese Conference on Artificial Intelligence* (pp. 711-722). Springer.
- Gamberini, L., Chittaro, L., & Paternò, F. (Eds.). (2012). *Human-Computer Interaction. I fondamenti dell’interazione tra persone e tecnologie*. London: Pearson.
- Gambhir, S. (2017, May 31). Chatbots: Opportunity and threat. *ComputerWorld*. Retrieved from <https://www.computerworld.com.au/article/620035/chatbots-opportunity-threat/>
- Gámez-Guadix, M., Orue, I., Smith, P. K., & Calvete, E. (2013). Longitudinal and reciprocal relations of cyberbullying with depression, substance use, and problematic internet use among adolescents. *The Journal of Adolescent Health*, 53(4), 446–452. doi:10.1016/j.jadohealth.2013.03.030 PMID:23721758
- Gammon, A. (2014). *Over a quarter of Americans have made malicious online comments*. YouGov.
- Gan, R., Neo, L. S., Chin, J., & Khader, M. (2018). *The psychology of hate: A case study analysis of the 2018 Sri Lanka Kandy Riots (HTBSC Research Report 18/2018)*. Singapore: Home Team Behavioural Sciences Centre.
- Ganti, V. (2018, June). The Role of Artificial Intelligence in Cybersecurity. *BizTech Magazine*.
- Gao, Y., Yang, M., Zhao, X., Pardo, B., Wu, Y., Pappas, T. N., & Choudhary, A. (2008, March). Image spam hunter. In *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on* (pp. 1765-1768). IEEE.
- Gao, H., Chen, Y., Lee, K., Palsetia, D., & Choudhary, A. N. (2012, February). Towards Online Spam Filtering in Social Networks. *NDSS*.

Compilation of References

- Gao, J. J., Rajan, B., Nori, R., Fu, B., Xiao, Y., & Liang, W. (2014). SCADA communication and security issues. *Security and Communication Networks*, 7(1), 175–194. doi:10.1002/ec.698
- Gardiner, J., & Nagaraja, S. (2016). On the Security of Machine Learning in Malware C&C Detection. *ACM Computing Surveys*, 49(3), 1–39. doi:10.1145/3003816
- Gareth, D. (2017). *Social media 'teen death groups' encouraging suicides sweep across Russia prompting 57 percent increase in youngsters taking their own lives*. Retrieved February 2018, from <http://www.dailymail.co.uk/news/article-4374978/Social-media-death-groups-prompts-57-rise-suicides.html#ixzz57Rb7E69z>
- Garfinkel, S. L. (2016). *Draft (2nd) NIST SP 800-188, De-Identification of Government Datasets*. Academic Press.
- Garfinkel, H. (2002). *Ethnomethodology's program: working out Durkheim's aphorism*. Lanham, MD: Rowman & Littlefield.
- Gascon, H., Uellenbeck, S., Wolf, C., & Rieck, K. (2014). *Continuous authentication on mobile devices by analysis of typing motion behavior*. GI Conference Sicherheit (Sicherheit, Schutz und Verlässlichkeit).
- Gaughan, A. J. (2017). Trump, Twitter, and the Russians: The Growing Obsolescence of Federal Campaign Finance Law. *Southern California Interdisciplinary Law Journal*, 27(1), 79–131. Retrieved from <https://ssrn.com/abstract=3069018>
- Gaydhani, A., Doma, V., Kendre, S., & Bhagwat, L. (2018). *Detecting Hate Speech and Offensive Language on Twitter using Machine Learning: An N-gram and TFIDF based Approach*. Retrieved from <https://arxiv.org/pdf/1809.08651.pdf>
- Gee, J., & Button, M. (2015). *The financial cost of healthcare fraud 2015 – what data from around the world shows*. London: PKK Littlejohn LLP. Retrieved from <http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/The-Financial-Cost-of-Healthcare-Fraud-Report-2015.pdf>
- Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, 18(7), 1219–1235.
- Gemmill, E., & Peterson, M. (2006). Technology use among college students: Implications for student affairs professionals. *NASPA Journal*, 43(2), 280–300. doi:10.2202/0027-6014.1640
- Geng, G. G., Li, Q., & Zhang, X. (2009, April). Link based small sample learning for web spam detection. In *Proceedings of the 18th international conference on World wide web* (pp. 1185–1186). ACM. 10.1145/1526709.1526920
- Genitsaridi, I., Kondylakis, H., Koumakis, L., Marias, K., & Tsiknakis, M. (2015). Evaluation of personal health record systems through the lenses of EC research projects. *Computers in Biology and Medicine*, 59, 175–185. doi:10.1016/j.combiomed.2013.11.004 PMID:24315661
- George, M. J., & Odgers, C. L. (2015). Seven Fears and the Science of How Mobile Technologies May Be Influencing Adolescents in the Digital Age. *Perspectives on Psychological Science*, 10(6), 832–851. doi:10.1177/1745691615596788 PMID:26581738
- Gerstenfeld, P. (2013). *Hate Crimes: Causes, Control and Controversies*. Sage Publications.
- Geser, H. (2002). Towards a (Meta-)Sociology of the Digital Sphere. In *Sociology in Switzerland: Towards Cyber-space and Vireal Social Relations*. Retrieved December 3, 2018, from http://socio.ch/intcom/t_hgeser13.htm
- Get Safe Online. (2018). Retrieved from <https://www.getsafeonline.org>
- Getoor, L., & Machanavajjhala, A. (2012). Entity resolution: Theory, practice & open challenges. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 5(12), 2018–2019. doi:10.14778/2367502.2367564

- Ghana News. (2018). *CID Arrests 12 suspects of a cybercrime syndicate*. Retrieved September 15, 2018, from Ghana News website: <http://ghananewsonline.com.gh/cid-arrests-12-suspects-cybercrime-syndicate/>
- Ghappour, A. (2017). Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. *Stanford Law Review*, 69, 1075–1136. Retrieved from https://repository.uchastings.edu/faculty_scholarship/1583
- Ghosh, A. & Nath, A. (2014). Cryptography Algorithms using Artificial Neural Network. *International Journal of Advance Research in Computer Science and Management Studies*, 2(11).
- Gibbs, S. (2018). Silk Road underground market closed – but others will replace it. *The Guardian*.
- Giechaskiel, I., Cremers, C., & Rasmussen, K. B. (Feb. 2016). On Bitcoin Security in the Presence of Broken Crypto Primitives. *European Symposium on Research in Computer Security (ESORICS 2016)*, 201-222. 10.1007/978-3-319-45741-3_11
- Gilbert, R. L., Murphy, N. A., & Ávalos, C. M. (2011, October). Communication Patterns and Satisfaction Levels in Three-Dimensional Versus Real-Life Intimate Relationships. *Cyberpsychology, Behavior, and Social Networking*, 14(10), 585–589. doi:10.1089/cyber.2010.0468 PMID:21381970
- Gilbert, R., Goldstein, H., & Hemingway, H. (2015). The market in healthcare data. *BMJ : British Medical Journal*, 351, h5897. doi:10.1136/bmj.h5897 PMID:26537618
- Giles, M. (2018, August 11). *AI for cybersecurity is a hot new thing—and a dangerous gamble*. Retrieved from Technology Review: <https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/>
- Gillespie, G. (2012). Guide to advising students about academic integrity. *The Mentor: An Academic Advising Journal*. Retrieved from <https://dus.psu.edu/mentor/2012/03/guide-to-advising-international-students-about-academic-integrity/>
- Gillespie, A. A. (2010). Defining Child Pornography: Challenges for the Law. *Child and Family Law Quarterly*, 22(2), 200–222.
- Gillespie, A. A. (2012). *Child pornography: Law and policy*. New York, NY: Routledge. doi:10.4324/9780203818107
- Gillespie, A. A. (2016). *Cybercrime: Key issues and debates*. New York, NY: Routledge.
- Gillies, D. (2014). Knowledge activism: Bridging the Research/Policy divide. *Critical Studies in Education*, 55(3), 272–288. doi:10.1080/17508487.2014.919942
- Gionis, A., Mazza, A., & Tassa, T. (2008). k-Anonymization revisited. In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on* (pp. 744–753). IEEE.
- github.com. (2018). *Smart-contract-best-practices*. Retrieved from <https://github.com/ConsenSys/smart-contract-best-practices>
- Gitonga, W. (2014). *The prevalence of internet crimes on women students at the University of Nairobi (Masters thesis)*. University of Nairobi. Retrieved from http://erepository.uonbi.ac.ke/bitstream/handle/11295/75135/Wanjiku_The%20prevalence%20of%20internet%20crimes%20on%20women%20students%20at%20the%20University%20of%20Nairobi.pdf?sequence=3&isAllowed=yhttp://erepository.uonbi.ac.ke/bitstream/handle/11295/75135/Wanjiku_The%20prevalence%20of%20internet%20crimes%20on%20women%20students%20at%20the%20University%20of%20Nairobi.pdf?sequence=3&isAllowed=y
- Gkoulalas-Divanis, A., Loukides, G., & Sun, J. (2014). Publishing data from electronic health records while preserving privacy: A survey of algorithms. *Journal of Biomedical Informatics*, 50, 4–19. doi:10.1016/j.jbi.2014.06.002 PMID:24936746

Compilation of References

- Glance, D. (2018). What is the Dark Web? *IFLScience*. Retrieved from <https://www.iflscience.com/technology/what-dark-web/all>
- Glasø, L., Nielsen, M. B., & Einarsen, S. (2009). Interpersonal Problems Among Perpetrators and Targets of Workplace Bullying. *Journal of Applied Social Psychology*, 39(6), 1316–1333. doi:10.1111/j.1559-1816.2009.00483.x
- Glenny, M. (2012). *DarkMarket: How hackers became the new media*. Vintage Books.
- Global Cybersecurity Index (GCI)*. (2017). International Telecommunication Union.
- GlobalSign. (2018). *What is SSL?* Retrieved from <https://www.globalsign.com/en-sg/ssl-information-center/what-is-ssl/>
- Goebert, D., Else, I., Matsu, C., Chung-Do, J., & Chang, J. Y. (2011). The impact of cyberbullying on substance use and mental health in a multiethnic sample. *Maternal and Child Health Journal*, 15(8), 1282–1286. doi:10.1007/10995-010-0672-x PMID:20824318
- Goffman, E. (1966). *Behavior in public places: notes on the social organization of gatherings*. New York: Free Press.
- Goh, Y. (2018). *Written Representations to the Select Committee on Deliberate Online Falsehoods; Effectiveness of Current Legislative Tools (Paper No. 129)*. Retrieved from Parliament of Singapore website: <https://www.parliament.gov.sg/docs/default-source/sconlinefalsehoods/written-representation-129.pdf>
- Goh, P., Tan, J., Neo, L. S., & Khader, M. (2017). *Understanding crowd behaviour during violent extremist attacks: Insights from the Nice truck attack 2016 (HTBSC Research Report 16/2017)*. Singapore: Home Team Behavioural Sciences Centre.
- Göktuna Yaylacı, F. (2012). Hukuk, Suç ve Toplum. In N. Suğur (Ed.), *Sosyolojiye Giriş* (pp. 167–202). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.
- Golbeck, J., Robles, C., & Turner, K. (2011). Predicting personality with social media. *Extended Abstracts on Human Factors in Computing Systems*, 253-262.
- Goldenberg, S. M., Silverman, J. G., Engstrom, D., Bojorquez-Chapela, I., & Strathdee, S. A. (2014). “Right here is the gateway”: Mobility, sex work entry and HIV risk along the Mexico-US border. *International Migration (Geneva, Switzerland)*, 52(4), 26–40. doi:10.1111/imig.12104 PMID:25346548
- Gold, M., & McLaughlin, C. (2016). Assessing HITECH Implementation and Lessons: 5 Years Later. *The Milbank Quarterly*, 94(3), 654–687. doi:10.1111/1468-0009.12214 PMID:27620687
- Goldman, D. (2013, January 31). Your antivirus software probably won't prevent a cyberattack. *CNN Tech*. Retrieved from <https://money.cnn.com/2013/01/31/technology/security/antivirus/index.html>
- Goldman, E. (2003). Warez trading and criminal copyright infringement. *J. Copyright Soc'y USA*, 51, 395.
- Goldstein, F. L., & Findley, B. F. (1996). *Psychological Operations: Principles and case studies*. Air Univ Maxwell AFB AL.
- Gomez-Cabrero, D., Abugessaisa, I., Maier, D., Teschendorff, A., Merckenschlager, M., Gisel, A., ... Tegnér, J. (2014). *Data integration in the era of omics: current and future challenges*. Academic Press.
- Gomm, R., Hammersley, M., & Foster, P. (2014). *Case Study Method: Key Issues, Key Texts*. Thousand Oaks, CA: Sage Publications.
- Good, O. S. (2018, October). Epic takes big-time YouTuber to federal court over Fortnite hacks. *Polygon*. Retrieved from <https://www.polygon.com/fortnite/2018/10/17/17991422/fortnite-hacks-lawsuit-golden-modz-youtube-takedown>

- Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. *Popular Communication*, 13(1), 74–86. doi:10.1080/15405702.2014.978000
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). *Explaining and Harnessing Adversarial Examples*. eprint arXiv:1412.6572v3
- Goodman, M. (2015). *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. Doubleday.
- Goodno, N. H. (2007). Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws. *Missouri Law Review*, 72(1), 1–74.
- Google. (2016). *Project Shield*. Retrieved from <https://www.google.com/ideas/products/project-shield/>
- Google. (2019). *Google Chrome*. Retrieved from https://www.google.com/chrome/?brand=CHBD&gclid=EAIaIQobChMI1L2JsqmB4AIVqrXtCh226QumEAAYASAAEgLzZvD_BwE&gclsrc=aw.ds
- Google+. (2018). *Collections*. Retrieved from <https://plus.google.com/discover>
- Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13–20. doi:10.1007/11416-006-0015-z
- Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to Information Security— Public Health Implications. *The New England Journal of Medicine*, 377(8), 707–709. doi:10.1056/NEJMp1707212 PMID:28700269
- Goswami, G., Ratha, N., Agarwal, A., Singh, R., & Vatsa, M. (2018). *Unravelling Robustness of Deep Learning based Face Recognition Against Adversarial Attacks*. eprint arXiv: 1803.00401v1
- Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.
- GovCERT.ch. (2016). *APT Case RUAG. Technical Report about the Espionage Case at RUAG*. Retrieved December 7, 2018, from https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf
- Government of Pakistan Bureau of Statistics. (2018). *Provisional Summary Results of 6th Population and Housing Census - 2017*. Retrieved from <https://bytesforall.pk/>
- Government of Pakistan. (2018). *National Response Centre for Cyber Crime*. Retrieved from <http://www.nr3c.gov.pk/cybercrime.html>
- Government of Pakistan. (n.d.). *Investigation for Fair Trial Act, 2013*. Retrieved from http://www.na.gov.pk/uploads/documents/1361943916_947.pdf
- Government of Pakistan. Ministry of Finance, Revenue & Economic Affairs. (2018). *Economic Survey of Pakistan, 2017*. Retrieved from http://www.finance.gov.pk/survey_1617.html
- Government of Pakistan. Ministry of Information Technology and Telecommunication. (2018). *Electronic Transactions Ordinance, 2002*. Retrieved from <http://www.pakistanlaw.com/eto.pdf>
- Government of Pakistan. Ministry of Information Technology and Telecommunication. (2018). *Prevention of Electronic Crimes Act, 2016*. Retrieved from http://www.na.gov.pk/uploads/documents/1470910659_707.pdf
- Gradinger, P., Strohmeier, D., & Spiel, C. (2009). Traditional bullying and cyberbullying. *The Journal of Psychology*, 217, 205–213.

Compilation of References

Graham, L. (2017, September 20). The number of devastating cyberattacks is surging – and it's likely to get much worse. *CNBC*. Retrieved from <https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html>

Graham, J., & Bowling, B. (1995). *Young People and Crime. Home Office Research Study 145*. London: Home Office. doi:10.1037/e450582008-001

Granville, K. (2018, March 19). Facebook and Cambridge Analytica: What you need to know as fallout widens. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., ... Theofanos, M. F. (2017). *Digital identity guidelines: authentication and lifecycle management*. doi:10.6028/NIST.SP.800-63b

Green, H. (2016, Oct. 4). How the Internet of Things will change (and improve) our everyday lives. *Forbes*. Retrieved from <https://www.forbes.com/sites/ibm/2016/10/04/how-the-internet-of-things-will-change-and-improve-our-everyday-lives/#712ec725374b>

Greenberg, A. (2013, November 8). Meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins. *Forbes*. Retrieved from <https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#637eb51f3d9b>

Greenberg, A. (2014). *Hacker Lexicon: What is the dark web?* Retrieved from <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>

Greenberg, A. (2018). *Operation Bayonet: Inside The Sting That Hijacked An Entire Dark Web Drug Market*. Retrieved from <https://www.wired.com/story/hansa-dutch-police-sting-operation/>

Greenberg, P. (2017). *The Newest Net Threat*. Retrieved from <http://www.ncsl.org/bookstore/state-legislatures-magazine/trends-in-state-policy-news.aspx#The%20Newest%20Net%20Threat>

Greenwood, C. (1983). The Relationship between ius ad bellum and ius in bello. *Review of International Studies*, 9(4), 221–234. doi:10.1017/S0260210500115943

Greig, J. (2018, April 19). Why human vulnerabilities are more dangerous to your business than software flaws. *TechRepublic*. Retrieved from <https://www.techrepublic.com/article/why-human-vulnerabilities-are-more-dangerous-to-your-business-than-software-flaws/>

Greijer, S., & Doek, J. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. Luxembourg: ECPAT.

Greiner, L. (2006). Hacking Your Network's Weakest Link. *netWorker Magazine*.

Grigg, D. W. (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. *Australian Journal of Guidance & Counselling*, 20(2), 143–156. doi:10.1375/ajgc.20.2.143

Grigg, D. W. (2012). Definitional constructs of cyberbullying and cyber aggression from a triagnulatory overview: A preliminary study into elements. *Journal of Aggression, Conflict and Peace Research*, 4(4), 202–215. doi:10.1108/17596591211270699

Grindr. (2018). *The World's largest social networking app for gay, bi, trans, and queer people*. Retrieved from <https://www.grindr.com/>

Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., & Dagon, D. (2007). Peer-to-peer botnets: Overview and case study. In N. Provos (Ed.), *HotBots*. USENIX Association.

- Gröndahl, T., Pajola, L., Juuti, M., Conti, M., & Asokan, N. (2018). *All You Need is Love: Evading Hate-speech Detection*. Retrieved from <https://arxiv.org/abs/1808.09115v1>
- Grover, J. (2018). State and USAID Should Improve Their Monitoring of International Counter-trafficking Projects. *GAO Reports*, 1–78. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=bth&AN=133416819&site=eds-live>
- Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies*, 43(5/6), 907–928. doi:10.1006/ijhc.1995.1081
- Gu, G., Zhang, J., & Lee, W. (2008). Botsniffer: Detecting botnet command and control channels in network traffic. NDSS The Internet Society.
- Guarineri, C. S. (2012). *a Tor-powered botnet straight from Reddit*. Academic Press.
- Guarino-Ghezzi, S., & Travino, A. J. (2005). *Understanding crime: A multidisciplinary approach*. New Providence, NJ: Matthew Bender & Company, Inc.
- Gu, G., Perdisci, R., Zhang, J., & Lee, W. (2008). Botminer: Clustering analysis of network traffic for protocol - and structure independent botnet detection. *USENIX Security Symposium*, 139–154.
- Guide to the Code of Conduct on Hate Speech - EDRI. (2018). Retrieved from <https://edri.org/guide-code-conduct-hate-speech/>
- Guinta, M., & John, R. (2018). Social media and adolescent health. *Pediatric Nursing*, 44, 196–201.
- Guldikova, I., Santagati, G. (2000). La mondialisation et la culture de participation. *Agora débats / jeunesse*, 19, 31–42.
- Gupta, N., Halevy, A. Y., Harb, B., Lam, H., Lee, H., Madhavan, J., . . . Yu, C. (2013, April). Recent progress towards an ecosystem of structured data on the Web. In *2013 IEEE 29th International Conference on Data Engineering (ICDE)* (pp. 5–8). IEEE. 10.1109/ICDE.2013.6544808
- Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247–267. doi:10.1007/11235-017-0334-z
- Gupta, D. S., & Biswas, G. P. (2016). Cryptanalysis of Wang et al.'s lattice-based key exchange protocol. *Perspectives on Science*, 8, 228–230. doi:10.1016/j.pisc.2016.04.034
- Gupta, D. S., & Biswas, G. P. (2017). A secure cloud storage using ECC-based homomorphic encryption. *International Journal of Information Security and Privacy*, 11(3), 54–62. doi:10.4018/IJISP.2017070105
- Gupta, S., Clements, B., Bhattacharya, R., & Chakravarti, S. (2004). Fiscal consequences of armed conflict and terrorism in low-and middle-income countries. *European Journal of Political Economy*, 20(2), 403–421. doi:10.1016/j.ejpoleco.2003.12.001
- Gupta, S., & Sharma, L. (2012). Exploitation of cross-site scripting (XSS) vulnerability on real world web applications and its defense. *International Journal of Computers and Applications*, 60(14), 28–33. doi:10.5120/9762-3594
- Guthrie, C. P., & Taylor, E. Z. (2017). Whistleblowing on Fraud for Pay: Can I Trust You? *Journal of Forensic Accounting Research*, 2(1), 1–19. doi:10.2308/jfar-51723
- Guzek, M., Bouvry, P., & Talbi, E.-G. (2015). A Survey of Evolutionary Computation for Resource Management of Processing in Cloud Computing [Review Article]. *IEEE Computational Intelligence Magazine*, 10(2), 53–67. doi:10.1109/MCI.2015.2405351

Compilation of References

- Gwern, B. (2015). *Dark Net Market archives, 2011-2015*. Retrieved from <https://www.gwern.net/DNM-archives>
- Gyongyi, Z., Berkhin, P., Garcia-Molina, H., & Pedersen, J. (2006, September). Link spam detection based on mass estimation. In *Proceedings of the 32nd international conference on Very large data bases* (pp. 439-450). VLDB Endowment.
- Haase, A. (2013). Harmonizing Substantive Cybercrime Law through European Union Directive 2013/40/EU – From European Legislation to International Model Law? *2015 First International Conference on Anti-Cybercrime (ICACC)*, 1-6. Retrieved May 15, 2019, from <https://ieeexplore.ieee.org/document/7351931>
- Haasz, A. (2016). Underneath it All: Policing International Child Pornography on the Dark Web. *Syracuse Journal of International Law and Commerce*, 43, 353–378.
- Haciyakupoglu, G., Hui, J. Y., Suguna, V., Leong, D., & Abdul Rahman, M. F. (2018). *Countering Fake News: A Survey of Recent Global Initiatives*. Retrieved from S. Rajaratnam School of International Studies website: <http://hdl.handle.net/11540/8063>
- Haddaji, R., Ouni, R., Bouaziz, S., & Mtibaa, A. (2016). Comparison of Digital Signature Algorithm and Authentication Schemes for H.264 Compressed Video. *International Journal of Advanced Computer Science and Applications*, 7(9), 2016. doi:10.14569/IJACSA.2016.070949
- Haddaway, N. R. (2015). The use of web-scraping software in searching for grey literature. *Grey J*, 11(3), 186–190.
- Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon (London)*, 3(7), e00346. doi:10.1016/j.heliyon.2017.e00346 PMID:28725870
- Hagan, F. E. (2013). *Introduction to criminology: Theories, methods and criminal behaviour* (8th ed.). London: Sage Publications Ltd.
- Haider, M. (2014, December 24). Political leaders reach consensus on military courts. *Dawn*. Retrieved from <https://www.dawn.com/news/1152909/political-leaders-reach-consensus-on-military-courts>
- Haider, I. (2018). Austrian law as a safe haven for foreign spies?: Analysis on the recent phenomenon of ‘Embassy Espionage’. *European Journal of Crime Criminal Law and Criminal Justice*, 25(3), 201–221. doi:10.1163/15718174-02603002
- Hakmeh, J. (2018). *Cybercrime Legislation in the GCC Countries: Fit for a Purpose?* International Security Department. London: Chatham House. Retrieved November 11, 2018, from <https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf>
- Halder, D. (2007, June). Cybercrime against women in India. *CyberLawTimes.com*. Retrieved from <http://www.cyber-lawtimes.com/articles/103.html>
- Halder, D., & Jaishankar, K. (2008). Cyber crimes against women in India: Problems, perspectives and solutions. *TMC Academic Journal*, 3(1), 48–62.
- Halder, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. *The Journal on Victimization*, 12(3), 5–26. Retrieved from <https://ssrn.com/abstract=1561774>
- Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders*, 6(4), 386–398. doi:10.1080/15564886.2011.607402
- Halder, D., & Jaishankar, K. (2012). *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations*; doi:10.4018/978-1-60960-830-9

- Halder, D., & Karuppannan, J. (2009). Cyber socializing and victimization of women. *Temida*, 12(3), 5–26. doi:10.2298/TEM0903005H
- Hale, S. (2014). Global Connectivity and Multilinguals in the Twitter Network. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY: ACM. 10.1145/2556288.2557203
- Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In *Proceedings of the IEEE International Symposium on Secure Software Engineering* (Vol. 1, pp. 13-15). IEEE.
- Hall, G. C., & Hirschman, R. (1991). Towards a theory of sexual aggression: A quadripartite model. *Journal of Consulting and Clinical Psychology*, 59(5), 662–669. doi:10.1037/0022-006X.59.5.662 PMID:1955601
- Hall, K. (2017). *Creating and Building Your Own Youtube Channel*. New York: Rosen Publishing Group.
- Hall, L., Aylett, R., & Paiva, A. (2009). FearNot!: providing children with strategies to cope with bullying. *Conference: Interaction Design and Children, Proceedings of the 8th International Conference on Interaction Design and Children, IDC 2009*.
- Halper, S. (2013). China: The three warfares. Report for the Office of Net Assessment, US Department of Defense.
- Han, Gupta, Tann, & Ong. (2018). *Towards Safer Smart Contracts: A Sequence Learning Approach to Detecting*. Academic Press.
- Hancock, D., & Algozzine, B. (2016). *Doing Case Study Research: A Practical Guide for Beginning Researchers*. New York: Teachers College Press.
- Handyside v. United Kingdom, 24 Eur. Ct. HR (set. A) at 23. (1976). Retrieved from http://www.coe.int/en/web/octopus/blog/-blogs/cyberhate-on-cyber-space-cyberbullying-a-new-phenomenon-of-violence-among-youth#_ftnref1
- Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., & Henry, J. (2017). *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Indianapolis, IN: Cisco Press.
- Han, H., Lu, X. L., Lu, J., Bo, C., & Yong, R. L. (2002). Data mining aided signature discovery in network-based intrusion detection system. *Operating Systems Review*, 36(4), 7–13. doi:10.1145/583800.583801
- Hanif, M. A. (2016). Exploration of cybercrime and cyber law: Growth of the state concerns and initiatives with special focus to the context of Bangladesh. *Prime University Journal of Multidisciplinary Quest*, 10(1), 1-22. Retrieved from http://www.primeuniversity.edu.bd/070513/journals/v_10_n_1_J_J_2016/Exploration.pdf
- Hansen, F. (2017). *Russian Hybrid Warfare: A study of Disinformation*. Danish Institute for International Studies (DIIS) Technical Report.
- Hansen, J., Saridakis, G., & Benson, V. (2017). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior*, 80, 197–206. doi:10.1016/j.chb.2017.11.010
- Hansen, L. (1982). Large Sample Properties of Generalized Method of Moments Estimators. *Econometrica*, 50(4), 1029–1054. doi:10.2307/1912775
- Hansen, L. L. (2009). Corporate financial crime: Diagnosis and treatment. *Journal of Financial Crime*, 16(1), 28–40. doi:10.1108/13590790910924948
- Hardaker, C., & McGlashan, M. (2016). Real men don't hate women: Twitter rape threats and group identity. *Journal of Pragmatics*, 91, 80–93. doi:10.1016/j.pragma.2015.11.005

Compilation of References

- Harlow, C. (2003). *Education and correctional populations. Bureau of Justice Statistics Special Report*. Washington, DC: U.S. Department of Justice.
- Harmony Labs (2017). *STAND UP – Virtual Reality to active bystanders against bullying Curriculum Guide*. Retrieved December 9, 2018, from Harmony Labs.org
- Harries, D., & Yellowlees, P. M. (2013). Cyberterrorism: Is the U.S. Healthcare System Safe? *Telemedicine Journal and e-Health*, 19(1), 61–66. doi:10.1089/tmj.2012.0022 PMID:23113795
- Harris, K. D. (2012). *The state of human trafficking in California*. California Department of Justice. Retrieved from <https://oag.ca.gov/sites/all/files/agweb/pdfs/ht/human-trafficking-2012.pdf>
- Harris, L.T. & Fiske, S.T. (2008). The Brooms in Fantasia: Neural Correlates of Anthropomorphizing Objects. *Social Cognition*, 26(2), 210-223. doi:10.1521/oco.2008.26.2.210
- Harris, D. (2019). Deepfakes: False Pornography Is Here and the Law Cannot Protect You. *Duke Law & Technology Review*, 17, 99–128.
- Hartnett, T. (2017, March 1). Meet the newest ethical and legal challenge of obtaining and using data via the internet: The dark web. *CenterWatch*. Retrieved from <https://www.centerwatch.com/news-online/2017/03/01/meet-the-newest-ethical-and-legal-challenge-of-obtaining-and-using-data-via-the-internet-the-dark-web/>
- Hasan, W. K. (2016, June). A survey of current research on Captcha. *International Journal of Computer Science & Engineering Survey*, 7(3), 21.
- Hassan, Y. (2017). *The illicit drug trade on the dark net: Analysing the need for a new EU Framework*. Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/51952/MAThesis_Yasmine_Hassan_s1750283.pdf?sequence=1
- Hatfield, J. M. (2017). Social Engineering in Cybersecurity: The Evolution of a Concept. *Computers & Security*.
- HatuqaD. (n.d.). Retrieved from <https://www.aljazeera.com/news/2015/09/algerian-hacker-hero-hoodlum-150921083914167.html>
- Haughn, M., & Gibilisco, S. (2017). *Confidentiality, Integrity, and Availability (CIA Triad)*. Retrieved from <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>
- HaveIBeenPwned. (n.d.). *Pwned websites. Breached websites that have been loaded into Have I Been Pwned*. Retrieve from <https://haveibeenpwned.com/PwnedWebsites/>
- Have, P. T. (2007). *Doing conversation analysis* (2nd ed.). Los Angeles, CA: SAGE. doi:10.4135/9781849208895
- Hayden, M. (2016, February 25). *The Encryption Wars And Privacy Shield*. Retrieved from <https://soundcloud.com/newamerica/the-encryption-wars-and-privacy-shield>
- Hayes, A. F., Glynn, C. J., & Shanahan, J. (2005). Validating the Willingness to Self-Censor Scale: Individual Differences in the Effect of the Climate of Opinion on Opinion Expression. *International Journal of Public Opinion Research*, 17(4), 443–455. doi:10.1093/ijpor/edh072
- Hayes, D., Cappa, F., & Cardon, J. (2018). A Framework for More Effective Dark Web Marketplace Investigations. *Information (Switzerland)*, 9, 186. doi:10.3390/info9080186
- Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, 9(4), 31–51. doi:10.1080/15536548.2013.10845689

- Hazelwood, R. R., & Warren, J. I. (2003). Linkage analysis: Modus operandi, ritual, and signature in serial sexual crime. *Aggression and Violent Behavior*, 8(6), 587–598. doi:10.1016/S1359-1789(02)00106-4
- HCCC. (2003). *Investigation report – Campbelltown and Camden hospitals, Macarthur Health Service*. Sydney: Health Care Complaints Commission. Retrieved from <https://trove.nla.gov.au/work/9673576?selectedversion=NBD25282706>
- Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, 48(3), 1–39.
- Hegadekatti, K. (2017). *Blockchain Technology - An Instrument of Economic Evolution?* SSRN Electronic Journal. doi:10.2139/ssrn.2943960
- Heider, F. (2015). *The Psychology of Interpersonal Relations*. Eastford, CT: Martino Fine Books. (Originally published 1958)
- Heintzelman, C. (2003). The Tuskegee Syphilis Study and Its Implications for the 21st Century. *The New Social Worker*, 10, 4. Retrieved from http://www.socialworker.com/feature-articles/ethics-articles/The_Tuskegee_Syphilis_Study_and_Its_Implications_for_the_21st_Century/
- Heiser, G., & Leslie, B. (2010, August). The OKL4 Microvisor: Convergence point of microkernels and hypervisors. In *Proceedings of the first ACM Asia-Pacific workshop on Workshop on systems* (pp. 19–24). ACM. 10.1145/1851276.1851282
- Helena Chiu, Y. T., Fang, S. C., & Tseng, C. C. (2010). Early versus potential adopters: Exploring the antecedents of use intention in the context of retail service innovations. *International Journal of Retail & Distribution Management*, 38(6), 443–459. doi:10.1108/09590551011045357
- Hendricks, D. (2013). Complete History of Social Media: Then and Now. *Small Business Trends*. Retrieved from <http://smallbiztrends.com/2013/05/thecomplete-history-of-social-media-infographic.html>
- Henzinger, M. (2007). Search technologies for the Internet. *Science*, 317(5837), 468–471. doi:10.1126/science.1126557 PMID:17656714
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. doi:10.1057/ejis.2009.6
- Herczeg, J. (2014). Actual problems of possession and viewing child pornography in Internet. *Jura*, 20(1), 70–80.
- Hernandez, A. E. (2000). Self-reported contact sexual offenses by participants in the Federal Bureau of Prisons Sex Offender Treatment Program: Implications for Internet sex offenders. Presented at the *19th Research and Treatment Conference of the Association for the Treatment of Sexual Abusers*, San Diego, CA.
- Herrera-Joancomartí, J. (2014). *Research and Challenges on Bitcoin Anonymity*. Springer International Publishing. doi:10.1007/978-3-319-17016-9_1
- Herrouz, A., Khentout, C., & Djoudi, M. (2013). *Overview of web content mining tools*. arXiv preprint arXiv:1307.1024.
- Hess, K., & Waller, L. (2014). The Digital Pillory: Media Shaming of ‘Ordinary People for Minor Crimes. *Continuum*, 28(1), 101–111. doi:10.1080/10304312.2013.854868
- Hewamadduma, S. I. (2017). Detection and prevention of possible unauthorized login attempts through stolen credentials from a phishing attack in an online banking system. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. 10.1109/ICRIIS.2017.8002440
- Hewilson. (2018). *The Deep Web: Statistics*. Retrieved from <https://hewilson.wordpress.com/what-is-the-deep-web/statistics/>

Compilation of References

- He, X., Qin, B., Zhu, Y., Chen, X., & Liu, Y. (2018). *SPESC: A specification language for smart contracts*. IEEE.
- He, Y., & Naughton, J. F. (2009). Anonymization of set-valued data via top-down, local generalization. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 2(1), 934–945. doi:10.14778/1687627.1687733
- Higgins, G. E. (2014). Understanding digital piracy using social networks. In C. D. Marcum & G. E. Higgins (Eds.), *Social Networking as a Criminal Enterprise*. Boca Raton, FL: CRC Press. doi:10.1201/b16912-10
- Hill, S. (2017, January 15). Is your smartphone listening to everything you say? We asked the experts. *Digital Trends*. Retrieved from <https://www.digitaltrends.com/mobile/is-your-smartphone-listening-to-your-conversations/>
- Hill, M. S., & Duncan, G. J. (1987). Parental family income and the socioeconomic attainment of children. *Social Science Research*, 16(1), 39–73. doi:10.1016/0049-089X(87)90018-4
- Hillman, H., Hooper, C., & Choo, K. K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review*, 30(6), 687–698. doi:10.1016/j.clsr.2014.09.007
- Hinduja, S., & Patchin, J. W. (2007). Offline consequences of online victimization. *Journal of School Violence*, 6(3), 89–112. doi:10.1300/J202v06n03_06
- Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29(2), 129–156. doi:10.1080/01639620701457816
- Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206–221. doi:10.1080/13811118.2010.494133 PMID:20658375
- Hinduja, S., & Patchin, J. W. (2012). Cyberbullying: Neither an epidemic nor a rarity. *European Journal of Developmental Psychology*, 9(5), 539–543. doi:10.1080/17405629.2012.706448
- Hinduja, S., & Patchin, J. W. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of Youth and Adolescence*, 42(5), 711–722. doi:10.1007/10964-012-9902-4 PMID:23296318
- Hinduja, S., & Patchin, W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence*, Vol. 31(1), 125–146. doi:10.1016/j.adolescence.2007.05.004 PMID:17604833
- HIPAA Privacy Rule and Its Impacts on Research. (2005). Retrieved from <https://privacyruleandresearch.nih.gov/healthservicesprivacy.asp>
- HIPAA. (2018). *When Was HIPAA Enacted? HIPAA (Health Insurance Portability and Accountability Act) | whatis.com*. (2017). Retrieved from <https://searchhealthit.techtarget.com/definition/HIPAA>
- Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Security*, 4(2), 2. doi:10.5038/1944-0472.4.2.1
- Hobbs, T. (2019). *Leviathan*. İstanbul: Yapı Kredi Yayınları.
- Hodges, J., Jackson, C., & Barth, A. (2018, January 31). *HSTS Policy*. HTTP Strict Transport Security (HSTS). IETF. doi:10.17487/RFC6797
- Hoffmann, J. (2006). *Stalking*. Heidelberg, Germany: Springer.
- Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values* (1st ed.). Beverly Hills, CA: Sage Publications.
- Hölbl, M., Welzer, T., & Brumen, B. (2012). An improved two-party identity-based authenticated key agreement protocol using pairings. *Journal of Computer and System Sciences*, 78(1), 142–150. doi:10.1016/j.jcss.2011.01.002

- Holmberg, R. J., Tlustý, M. F., Futoma, E., Kaufman, L., Morris, J. A., & Rhyne, A. L. (2015). The 800-pound grouper in the room: Asymptotic body size and invasiveness of marine aquarium fishes. *Marine Policy*, 53, 7–12. doi:10.1016/j.marpol.2014.10.024
- Holsapple, C. W., & Joshi, K. (2004). A formal knowledge management ontology: Conduct, activities, resources, and influences. *Journal of the American Society for Information Science and Technology*, 55(7), 593–612. doi:10.1002/asi.20007
- Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, 46(1), 189–220. doi:10.1111/j.1745-9125.2008.00101.x
- Holt, M. K., & Espelage, D. L. (2007). Perceived Social Support among Bullies, Victims, and Bully-Victims. *Journal of Youth and Adolescence*, 36, 984–994. doi:10.1007/10964-006-9153-3
- Holt, M., & Keyes, M. (2004). Teachers' attitudes toward bullying. In D. Espelage & S. Swearer (Eds.), *Bullying in American schools: A social-ecological perspective on prevention and intervention* (pp. 121–139). Mahwah, NJ: Erlbaum.
- Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20–40. doi:10.1080/01639625.2013.822209
- Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. New York: Routledge Press.
- Holtz, M., David, B., Deus, F. E., de Sousa, R. T., Jr., & Laerte, P. (2011). *A formal classification of Internet Banking Attacks and vulnerabilities*. Academic Press.
- HomeBorderCtrl. (2018). Retrieved from <https://www.iborderctrl.eu/>
- Homeland Security Act (HSA) (2002). Pub. L. No. 197, 116 Stat. 2135.
- Hoofnagle, C., Urban, J., & Li, S. (2012). Privacy and Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection of Data about their Online Activities. *Amsterdam Privacy Conference. HTTP cookies*. Retrieved from Mozilla Developer Network: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>
- Hootsuite. (2018). *The global state of digital in 2018—from Argentina to Zambia*. Author.
- Horacek, S. (2018, April). You wanna see something wild? Check out all the advertisers targeting you on Facebook. *Popular Science*. Retrieved from <https://www.popsci.com/advertisers-targeting-facebook-account-settings>
- Horne, B. & Adali, S. (2017). *This just in: fake news pack a lot in title, uses simple, repetitive content in text body, more similar to satire than real news*. ArXiv, 1703.09398
- Ho, S. S., & McLeod, D. M. (2008). Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication. *Communication Research*, 35(2), 190–207. doi:10.1177/0093650207313159
- Ho, S. S., & Ng, V. T. (1994). Customers' Risk Perceptions of Electronic Payment Systems. *International Journal of Bank Marketing*, 12(8), 26–38. doi:10.1108/02652329410069029
- Hossein Hassani, X. H. (2018, July 20). *Digitalisation and Big Data Mining in Banking*. Academic Press.
- Hovy, E., Bryan, N. M., Philpot, A., Silva, D. R., & Sundararajan, A. (2014). Data Integration from Open Internet Sources and Network Detection to Combat Underage Sex Trafficking. In *Proceedings of the 15th Annual Internet International Conference on Digital Government Research*, (pp. 86-90). New York, NY: Association for Computing Machinery.

Compilation of References

- Howard, P. N., Ganesh, B., Liotsu, D., Kelly, J., & Francois, C. (2018). *The IRA, Social Media and Political Polarization in the United States, 2012-2018*. Computational Propaganda Research Project. University of Oxford. Retrieved from <https://comprop.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf>
- Howard, J. D. (1997). *An analysis of security incidents on the Internet 1989-1995*. Carnegie-Mellon Univ Pittsburgh PA.
- Howard, P. (2009). *What is scenography?* (2nd ed.). London: Routledge.
- Howe, A. (2017, November 8). *Legal Age of Consent in All 50 States*. Retrieved from <https://www.thesurvivoralliance.com/forallies/legal-age-consent-50-states/>
- Howells, K. (1994). Child sexual abuse: Finkelhor's precondition model revisited. *Psychology, Crime & Law*, 1(3), 201–214. doi:10.1080/10683169508411956
- Huang, Y., & Chou, C. (2010). An analysis of multiple factors of cyberbullying among junior high school students in Taiwan. *Computers in Human Behavior*, 26(6), 1581–1590. doi:10.1016/j.chb.2010.06.005
- Huber, E., & Pospisil, B. (2017). *Die Cyber-Kriminellen in Wien. Eine Analyse von 2006-2016*. Krems an der Donau: tredition GmbH.
- Huber, E., Pospisil, B., & Seböck, W. (2018). Without a trace - Cybercrime how are the offenders. In *DeepSec*. Retrieved from https://www.researchgate.net/publication/329321526_Without_a_Trace-Cybercrime_Who_are_the_Offenders
- Huber, E., Pospisil, B., Hötendorfer, W., Quirchmayr, G., Löschl, L., & Tschohl, C. (2018). *Die Cyber-Kriminellen in Wien: Eine Analyse von 2006-2016*. Krems an der Donau: Tredition.
- Huber, E. (2012). *Cyberstalking und Cybercrime - kriminalsoziologische Untersuchung zum Cyberstalking-Verhalten der Österreicher*. Wiesbaden: Springer.
- Huber, E. (2019). *Cybercrime - Eine Einführung*. Wiesbaden: Springer. doi:10.1007/978-3-658-26150-4
- Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards automating social engineering using social networking sites. In *Proceedings of the 2009 International Conference on Computational Science and Engineering* (Vol. 3, pp. 117-124). 10.1109/CSE.2009.205
- Huber, M., Mulazzani, M., Schrittwieser, S., & Weippl, E. (2010). Cheap and automated socio-technical attacks based on social networking sites. *Proceedings of the 3rd Workshop on Artificial Intelligence and Security AISec2010*. 10.1145/1866423.1866435
- Hughes, C. (2019, May 12). It's Time to Break Up Facebook. *New York Times*, p. SR1.
- Hughes, K., Lecky-Thompson, J., Ammon, M., & Murphy, H. (2017). *Track the impact of your publications*. Academic Press.
- Huling, A. (2012). Domestic Workers in Malaysia: Hidden Victims of Abuse and Forced Labor. *New York University Journal of International Law & Politics*. New York University. *International Law Society*, 44(2), 629. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edb&AN=74646207&site=eds-live>
- Hultgren, M., Jennex, M. E., Persano, J., & Ornatowski, C. (2016, January). Using knowledge management to assist in identifying human sex trafficking. In *System Sciences (HICSS), 2016 49th Hawaii International Conference on* (pp. 4344-4353). IEEE. 10.1109/HICSS.2016.539
- Hunt, E. (2017). *Higher proportion of men than women report online abuse in survey*. Retrieved from <https://www.theguardian.com/media/2016/sep/06/higher-proportion-of-men-than-women-report-online-abuse-in-survey>

- Hunt, T. (2016, October). *Handling Chinese data breaches in Have I Been Pwned*. Retrieved from <https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/>
- HuntSource. (2018, January 15). Cyber security and the Dark Web. *HuntSource*. Retrieved from <https://huntsource.io/cyber-security-dark-web/>
- Hurlburt, G. (2017). Shining Light on the Dark Web. *Computer*, 50(4), 100–105. doi:10.1109/MC.2017.110 PMID:29213147
- Hussain, M. A., Jin, H., Hussien, Z. A., Abduljabbar, Z. A., Abbdal, S. H., & Ibrahim, A. (2016). DNS Protection against Spoofing and Poisoning Attacks. *Information Science and Control Engineering (ICISCE) 2016 3rd International Conference on*, 1308-1312. 10.1109/ICISCE.2016.279
- Hussain, G., & Saltman, E. M. (2014). *Jihad trending: A comprehensive analysis of online extremism and how to counter it*. London: Quilliam Foundation.
- Husserl, E. (1976). *Die Krisis der europäischen Wissenschaften und die transzendente Phänomenologie. Eine Einleitung in die phänomenologische Philosophie* (Vol. 6). Den Haag: Husserliana. doi:10.1007/978-94-010-1335-2
- Hutchings, A. (2013). *Theory and crime: Does it compute?* Griffith University.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2010). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. White Paper from the Lockheed Martin Corporation. Retrieved December 7, 2018, from <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
- Hu, Y., Shin, J., & Tang, Z. (2013). *Performance-based Pricing Models in Online Advertising: Cost per Click versus Cost per Action*. Atlanta, GA: Georgia Institute.
- Hymas, C. (2018). *Legal system fails to protect women from online abuse, says Law Commission*. Retrieved 12th of November 2018 from <https://www.telegraph.co.uk/news/2018/11/01/legal-system-fails-protect-women-online-abuse-says-law-commission/>
- Ibanez, M., & Suthers, D. D. (2014). Detection of domestic human trafficking indicators and movement trends using content available on open Internet sources. In *Proceedings of the Hawaii International Conference on System Sciences* (pp. 1556-1565). 10.1109/HICSS.2014.200
- Iberahima, H., Husseinb, N., Samatc, N., Noordind, F., & Daude, N. (2013). Academic dishonesty: Why business students participate in these practices? *Social and Behavioral Sciences*, 90, 152–156.
- IBM. (2018). *2018 Cost of a Data Breach Report: Global Overview*. Ponemon Institute.
- Idoko, N. A., & Ugwuanyi, R. N. C. (2015). *Cyber Crimes: Bane of Nigeria's Information Growth and Utilization*. Retrieved from www.jaistonline.org
- Ifenkwe, G. E. (2013). Educational development in Nigeria: Challenges and prospects in the 21st century. *Universal Journal of Education and General Studies*, 2(1), 7–14.
- ILO (International Labour Office). (2009). *Global Employment Trends 2009*. Geneva: International Labour Office.
- IMPACT. (2012). *IMPACT: International MUltilateral Partnership Against Cyberthreats*. Retrieved November 22, 2018, from ITU: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- Ingraham, N. (2017, March 12). Building your own chatbot is a lot easier than you'd expect. *Engadget*. Retrieved from <https://www.engadget.com/2017/03/12/build-your-own-chatbot-hands-on/>

Compilation of References

- Instagram. (2018). *Sign up to see photos and videos from your friends*. Retrieved from <https://www.instagram.com/>
- INTEGRAL. (2010). AIM -Austrian Internet Monitor, rep. Österr. ab 14 Jahren, April bis Juni 2010, n= 3 000 pro Quartal. Wien: Author.
- INTEGRAL. (2018). AIM 2. *Quartal/2018*. Retrieved from https://www.integral.co.at/downloads/Internet/2018/07/AIM-C_-_Q2_2018.pdf
- Intelliagg. (2016). *Deeplight: Shining a light on the dark web*. Author.
- Intelliagg. (2016). *Deeplight: Shining A Light On The Dark Web*. London: Intelliagg.
- International Monetary Fund. (2018). *World Economic Outlook Database*. Retrieved May 15, 2019, from <https://www.imf.org/external/pubs/ft/weo/2018/02/weodata/weorept.aspx?pr.x=42&pr.y=2&sy=2019&ey=2023&scsm=1&ssd=1&sort=country&ds=.&br=1&c=998&s=NGDP%20D%20PPP%20GDP%20PPP%20C&grp=1&a=1>
- International Telecommunication Union (ITU). (2017, July 6). *Global Cybersecurity Index 2017*. Retrieved from <https://www.itu.int/en/ITU-D/Pages/publications.aspx#/publication/59dae8cf13659441249d2fa9>
- International Telecommunications Union. (n.d.). Retrieved November 28, 2018, from [https://media.scmagazine.com/documents/224/deeplight_\(1\)_55856.pdf](https://media.scmagazine.com/documents/224/deeplight_(1)_55856.pdf)
- Internet Watch Foundation. (2018). *Trends in Online Child Sexual Exploitation: Examining the Distribution of Live-streamed Child Sexual Abuse*. Retrieved from <https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf>
- Internet World Stats. (2018). *Internet usage statistics: The internet big picture world internet users and 2018 population stats*. Retrieved from <https://www.internetworldstats.com/stats.htm>
- Internet World Stats. (2018). Retrieved from <https://www.internetworldstats.com/asia/pk.htm>
- Internet World Stats. (2018). *World Statistics*. Retrieved October 12, 2018, from <http://www.internetworldstats.com/stats1.htm>
- Internet World Stats. (2019). *Internet Usage Statistics*. Accessed on June 16, 2019. <https://www.internetworldstats.com/stats.htm>
- Interpol. (2017, March). *Collective Action Against Cybercrime*. Retrieved November 21, 2018, from <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKEwjshOjXtfHeAhVIqI8KHdedBf8QFjAIegQIARAC&url=https%3A%2F%2Fwww.interpol.int%2FMedia%2FFiles%2FAbout-INTERPOL%2FIGCI%2FInformation-Sheets%2FCollective-action-against-cybercrime%2F&usq>
- Interpol. (n.d.). Retrieved from <https://www.interpol.int/crime-areas/cybercrime/cybercrime>
- ISAB. (2017). *Report on Gray Zone Conflict*. Retrieved from <https://www.state.gov/t/avc/isab/266650.html>
- Isdal, T., Piatek, M., Krishnamurthy, A., & Anderson, T. (2011). Privacy-preserving p2p data sharing with oneswarm. *Computer Communication Review*, 41(4), 111–122. doi:10.1145/1851275.1851198
- Isidore, C., & Gaouette, N. (2018). US charges Chinese hackers in global scheme targeting business and military. *CNN*. Retrieved from <https://www.cnn.com/2018/12/20/tech/chinese-hacker-charges/index.html>
- Isikoff, M., & Corn, D. (2018). *Russian Roulette: The Inside Story of Putin's War on American and the Election of Donald Trump*. New York: Hatchette Book Group.

- Ismail, K. A., Singh, M. M., Mustafa, N., Keikhosrokiani, P., & Zulkefli, Z. (2017). Security Strategies for Hindering Watering Hole Cyber Crime Attack. *Procedia Computer Science*, 124, 656–663. doi:10.1016/j.procs.2017.12.202
- ISO/IEC 27002:2013. Information technology -- Security techniques -- Code of practice for information security controls.
- Iswaran, S. (2018, August 6). Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity, on the cyber-attack on SingHealth's IT system, during Parliamentary Sitting, 6 August 2018. *Ministry of Communications and Information*. Retrieved from <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/8/statement-by-mr-s-iswaran-on-cyber-attack-on-singhealth-it-system-during-parl-sitting-on-6-aug-2018>
- ITU. (2012). *Understanding cybercrime: Phenomena, challenges and responses*. Geneva: International Telecommunication Union. Retrieved November 29, 2018, from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- ITU. (2015). Global Cybersecurity Index & Cyberwellness Profiles. In 4. *Lain-Lain*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- ITU. (2017). *Global Cybersecurity Index (GCI) 2017*. Geneva: International Telecommunication Union.
- Ivaschenko, A. I. (2016). Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to Improve their Investment Attractiveness. *Problèmes Économiques*, (3): 267–273.
- Jack, J. T. C. B., & Ene, R. W. (2016). Cybercrime and the Challenges of Socio-economic Development in Nigeria. *JORIND*, 14(2), 42–49.
- Jacobs, N., Vollink, T., Dehue, F., & Lechner, L. (2014). Online Pestkoppenstoppen: Systematic and theory-based development of a web-based tailored intervention for adolescent cyberbully victims to combat and prevent cyberbullying. *BMC Public Health*, 14(1), 396. doi:10.1186/1471-2458-14-396 PMID:24758264
- Jacoby, J. (2018). *The Facebook Dilemma*. Public Broadcasting Service.
- Jaha, F., & Kartit, A. (2017). Pseudo code of two-factor authentication for BYOD. *2017 International Conference on Electrical and Information Technologies (ICEIT), IEEE Conferences*, 1 – 7.
- Jahangir, R. (2018, October 28). Pakistan's online clampdown. *Dawn*. Retrieved from <https://www.dawn.com/news/1441927>
- JainM. (2018, May 30). Retrieved from https://www.business-standard.com/article/economy-policy/at-18-indian-customers-biggest-victims-of-banking-fraud-fis-study-118052900467_1.html
- Jaishankar, K. (2008). Space transition theory of cyber crimes. *Crimes of the Internet*, 283–301.
- Jakobsson, M. (2016). *Understanding social engineering based scams*. Springer. doi:10.1007/978-1-4939-6457-4
- Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2017). *Internet of Things (IoT) promises new benefits—and risks: A systematic analysis of adoption dynamics of IoT products*. Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. Working Paper CISL#2017-15. Retrieved from <http://web.mit.edu/smadnick/www/wp/2017-15.pdf>
- James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, 26(2), 107–122. doi:10.1080/08946566.2013.821809 PMID:24499279
- James, G. (2000). The price of privacy. *Upside.*, 12(4), 182–190.
- Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, 5(4), 87–88. doi:10.4103/0976-0105.141942 PMID:25316987
- Janda, J. (2016). *The Lisa Case STRATCOM Lessons for European states*. Federal Academy for Security Policy Working Paper No.11/2016.

Compilation of References

- Jang, H., Song, J., & Kim, R. (2014). Does the offline bully-victimization influence cyberbullying behavior among youths? Application of general strain theory. *Computers in Human Behavior*, 31, 85–93. doi:10.1016/j.chb.2013.10.007
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cyber security. *Journal of Computer and System Sciences*, 80(5), 973–993. doi:10.1016/j.jcss.2014.02.005
- Jang, S., & Kim, J. (2018). Third person effects of fake news: Fake news regulation and media literacy interventions. *Computers in Human Behavior*, 80, 295–302. doi:10.1016/j.chb.2017.11.034
- Jánoskúti, B. (2016). Take down and blocking measures (Art. 25 & recitals 46–47). In *Survey on the transposition of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography*. Retrieved from: <http://missingchildreneurope.eu/Portals/0/Docs/A%20survey%20on%20transposition%20of%20Directive%20against%20child%20sexual%20exploitation%20and%20abuse.pdf>
- Jansen, F., Koops, B., Lenthe, J. v., Maas, E., Planken, E., Schermer, B., . . . Verhoeven, M. (2017). Tackling Cybercrime. In *Research Agenda. The human factor in Cybercrime and Cybersecurity*, (pp. 55–64). Eleven International Publishing.
- Jansen, J., & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In *Socio-Technical Aspects in Security and Trust (STAST)*, 2015 Workshop on (pp. 24–31). IEEE.
- Jarboe, G. (2011). *YouTube and Video Marketing: An Hour a Day* (2nd ed.). Sybex.
- Jardine, E. (2015). *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Center for International Governance Innovation and Chatham House.
- Jaschik, S. (2014, September 15). Interview with professor fired by West Bank university who compares himself to Steven Salaita. Inside Higher Ed. Retrieved from <https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita>
- Jay, J. (2018, March 31). Hackers still exploiting the human factor to carry out ransomware attacks. *SC Media*. Retrieved from <https://www.scmagazineuk.com/hackers-exploiting-human-factor-carry-ransomware-attacks/article/1472956>
- Jayakumar, S. (2018). *Germany's NetzDG: Template for Dealing with Fake News?* S. Rajaratnam School of International Studies.
- Jeanniere, A. (1993). Modernite Nedir? In M. Küçük (Ed.), *Modernite versus Postmodernite* (pp. 95–132). Ankara: Vadi Yayınları.
- Jeet, S. (2012). Cyber crimes against women in India: Information technology act, 2000. *Elixir International Journal Elixir Criminal Law*, 47, 8891–8895.
- Jegede, A. E., Adejuwon, G. A., Olowookere, E. I., & Elegbeleye, A. O. (2016). Ecological Approach to Nigerian Youths Cyber-Fraud Participation. *Social Sciences*, 11(22), 5284–5293.
- Jegede, A. E. (2016). Modern Technology, Global Risk and the Challenges of Crime in the Era of Late Modernity. In N. Okorie, B. R. Ojebuyi, & A. Salawu (Eds.), *Impact of the Media on African Socio-Economic Development* (pp. 18–32). IGI Books Publication.
- Jegede, A. E., Ajayi, M. P., & Allo, T. (2016). Risk and investment decision making in technological age: A dialysis of cyber fraud complication in Nigeria. *International Journal of Cyber Criminology*, 10(1), 62–78.
- Jenab, K., Khoury, S., & LaFavor, K. (2018). Flow-Graph and Markovian Methods for Cyber Security Analysis. In I. Management Association (Ed.), *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 674–702). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-5634-3.ch036

- Jenab, K., Khoury, S., & LaFevor, K. (2016). Flow-Graph and Markovian Methods for Cyber Security Analysis. *International Journal of Enterprise Information Systems*, 12(1), 59–84. doi:10.4018/IJEIS.2016010104
- Jeney, P. (2015). *Combating child sexual abuse online*. Study for the LIBE Committee. Retrieved from: [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536481/IPOL_STU\(2015\)536481_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536481/IPOL_STU(2015)536481_EN.pdf)
- Jenkins, H. (2006). *Convergence Culture. La cultura de la convergencia de los medios de comunicación*. Barcelona: Paidós.
- Jennex, M. E. (2005). What is knowledge management? *International Journal of Knowledge Management*, 1(4), i–iv.
- Jennex, M. E. (2017). Big data, the Internet of things and the revised knowledge pyramid. *The Data Base for Advances in Information Systems*, 48(4), 69–79. doi:10.1145/3158421.3158427
- Jennex, M. E., & Bartczak, S. E. (2013). A revised knowledge pyramid. *International Journal of Knowledge Management*, 9(3), 19–30. doi:10.4018/ijkm.2013070102
- Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of internet users: Self- reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2), 203–227. doi:10.1016/j.ijhcs.2005.04.019
- Jeong, I. R., Katz, J., & Lee, D. H. (2004, June). One-round protocols for two-party authenticated key exchange. In *International Conference on Applied Cryptography and Network Security* (pp. 220-232). Springer. 10.1007/978-3-540-24852-1_16
- Jiang, D. (2011). Security issues in massively multiplayer online games. *ACC 626 Research Paper*. Retrieved from <http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Security%20Issues%20in%20Massively%20Multiplayer%20Online%20Games%20X%20Jiang.pdf>
- Jiang, H., Emmerton, L., & McKauge, L. (2013). Academic integrity and plagiarism: A review of the influences and risk situations for health students. *Higher Education Research & Development*, 32(3), 369–380. doi:10.1080/07294360.2012.687362
- Jia, R., & Liang, P. (2017). Adversarial Examples for Evaluating Reading Comprehension Systems. *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing* (pp. 2021-2031). Copenhagen, Denmark: Association for Computational Linguistics. 10.18653/v1/D17-1215
- Jin, Z., Cao, J., Zhang, Y., & Luo, J. (2016). News verification by exploiting conflicting social viewpoints in microblogs. In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*. AAAI Press.
- John, R. (2016, March). Outsourcing fun: Gold farming & the rise of digital sweatshops. *The Online Economy*. Retrieved from <https://onlineeconomy.hbs.org/submission/outsourcing-fun-gold-farming-the-rise-of-digital-sweatshops/>
- Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. *NIST Special Publication 800-150, Computer Security*. Retrieved May 16, 2019, from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>
- Johnson, D., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, 48(5), 1367. doi:10.2307/1229390
- Johnson, F., & Gupta, S. K. (2012). Web content mining techniques: A survey. *International Journal of Computers and Applications*, 47(11).
- Johnson, J. R. (1978). The Authenticity and Validity of Antony's will. *L'Antiquite Classique*, 47(2), 494–503. doi:10.3406/antiqu.1978.1908

Compilation of References

- Joinson, A. (1998). Causes and implications of behavior on the Internet. In J. Gackenbach (Ed.), *Psychology and the Internet: Intrapersonal, interpersonal, and transpersonal implications* (pp. 43–60). San Diego, CA: Academic Press.
- Jones, C. W. (2005, April). *Council of Europe Convention on Cybercrime: Themes and critiques*. Workshop on the International Dimensions of Cyber Security. Hosted by Georgia Institute of Technology and Carnegie Mellon University.
- Jordan, T., & Taylor, P. A. (1998). Sociology of Hackers. *The Sociological Review*, 46(4), 757–781. doi:10.1111/1467-954X.00139
- Josang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2), 618–644. doi:10.1016/j.dss.2005.05.019
- Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., & Arab, M. (2014). Using data mining to detect health care fraud and abuse: A review of literature. *Global Journal of Health Science*, 7(1), 194–202. doi:10.5539/gjhs.v7n1p194 PMID:25560347
- Ju, J., Cho, D., Lee, J. K., & Ahn, J.-H. (2016). *An Empirical Study on Anti-spam Legislation*. Academic Press.
- Jung, Y., Chun, S.A., & Geller, J. (2008). Toward the Semantic Deep Web. *Computer*, 95-97. doi:10.1109/MC.2008.402
- Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75–87. doi:10.1016/j.chb.2016.09.012
- Jung, S., Ahn-Redding, H., & Allison, M. (2014). Crimes and punishment: Understanding of the criminal code. *Canadian Journal of Criminology and Criminal Justice*, 56(3), 341–366. doi:10.3138/cjccj.2013.E17
- Jung, Y., Leventhal, B., Shin Kim, Y., Park, T. W., Lee, S., Lee, M., ... Park, J. (2014). Cyberbullying, Problematic Internet Use, and Psychopathologic Symptoms among Korean Youth. [English.]. *Yonsei Medical Journal*, 55(3), 826–830. doi:10.3349/ymj.2014.55.3.826 PMID:24719154
- Juniper Networks. (2014). *Human trafficking in Silicon Valley*. Retrieved from <https://flipflashpages.uniflip.com/3/88537/339160/pub/html5.html#page/1>
- Jurasz, O., & Barker, K. (2017). Submission of Evidence to Scottish Government Independent Review of Hate Crime Legislation (Bracadale Review). *Independent Review of Hate Crime Legislation in Scotland*. Retrieved 12th of November 2018 from <http://oro.open.ac.uk/52612/1/Hate%20Crime%20Legislation%20Review%20%28Barker%20%26%20Jurasz%29.pdf>
- Jurisica, I., Mylopoulos, J., & Yu, E. (1999). Using ontologies for knowledge management: An information systems perspective. In *Proceedings of the Annual Meeting-American Society for Information Science* (vol. 36, pp. 482-496). Academic Press.
- Jusoh, S. (2016). *Cyber Related Policies and Laws in Malaysia*. Retrieved December 2, 2018 from <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-related-policies-and-laws-malaysia>
- Kabir, N. (2018). *Cybercrime a new form of violence against women: From the case study of Bangladesh*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3153467
- Kaczynski, T. (1995). *Industrial society and its future*. Retrieved from <http://editions-hache.com/essais/pdf/kaczynski2.pdf>
- Kajzer, M. D., Crowell, C. R., Villano, M., Zenk, J., Segerson, J., Behrens, N., & Battis, N. (2019in press). Building word-level models from chat dialogue to distinguish sexual offenders from victims and to differentiate among offender types. In R. Johnson (Ed.), *Digital Innovations in Criminal Science Investigations and Forensics*. Hershey, PA: IGI-Global.

- Kals, S., Kirda, E., Kruegel, C., & Jovanovic, N. (2006, May). Secubat: a web vulnerability scanner. In *Proceedings of the 15th international conference on World Wide Web* (pp. 247-256). ACM. 10.1145/1135777.1135817
- Kamal, M. M., Chowdhury, I. A., Haque, N., Chowdhury, M. I., & Islam, M. N. (2012). Nature of cybercrime and its impacts on young people: A case from Bangladesh. *Asian Social Science*, 8(15), 171–183. doi:10.5539/ass.v8n15p171
- Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E. (2014). Introducing touchstroke: Keystroke-based authentication system for smartphones. *Security and Communication Networks*.
- Kamini, D. (2011). Cyber Crime in the Society. *Problems and Preventions Journal of Alternative Perspectives in the Social Sciences*, 3(1), 240–259.
- Kanat-Maymon, Y., Almog, L., Cohen, R., & Amichai-Hamburger, Y. (2018). Contingent self-worth and Facebook addiction. *Computers in Human Behavior*, 88, 227–235. doi:10.1016/j.chb.2018.07.011
- Kang, C. (2012). Megaupload shutdown raises new internet-sharing fears. *The Washington Post*.
- Kang, J., & Lee, D. (2007). Advanced white list approach for preventing access to phishing sites. *Convergence Information Technology, 2007. International Conference 2007*, 491–496. 10.1109/ICCIT.2007.50
- Kang, R. (2018, January 23). Welcome to the dark Web: A plain English introduction. *IAPP*. Retrieved from <https://iapp.org/news/a/welcome-to-the-dark-web-a-plain-english-introduction/>
- Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). “My data just goes everywhere”: User mental models of the internet and implications for privacy and security. *Eleventh Symposium on Usable Privacy and Security*, 39-52. Retrieved from <https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf>
- Kansky, K., Silver, T., Mély, D. A., Eldawy, M., Lázaro-Gredilla, M., Lou, X., . . . George, D. (2017). Schema Networks: Zero-shot Transfer with a Generative Causal Model of Intuitive Physics. *Thirty-fourth International Conference on Machine Learning*. Retrieved from <http://proceedings.mlr.press/v70/kansky17a/kansky17a.pdf>
- Kapell, A. (2009). *Sexual Exploitation of Children in Tourism*. ECPAT International. Retrieved from http://www.ecpat.org/wp-content/uploads/legacy/Child-Friendly_Child%20Sex%20Tourism_2009.pdf
- Kaplan, M., & Haenlein, I. (2009). *Users of the world, unite! The media challenges opportunities of social media*. Kelly school of Business, Indiana University.
- Kaplan, A. M., & Haenlein, M. (2010). Users of the World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons*, 53(1), 59–68. doi:10.1016/j.bushor.2009.09.003
- Kaplan, S. E. Jr, & Schultz, J. Jr. (2007). Intentions to report questionable acts: An examination of the influence of anonymous reporting channel, internal audit quality and setting. *Journal of Business Ethics*, 71(2), 109–124. doi:10.1007/10551-006-0021-6
- Kaptein, M. (2011). From Inaction to External Whistleblowing: The Influence of the Ethical Culture of Organizations on Employee Responses to Observed Wrongdoing. *Journal of Business Ethics*, 98(3), 513–530. doi:10.1007/10551-010-0591-1
- Karadağ, A. (2006). Kamusal Alan Modelleri Çoğulcu Perspektiften Bir Değerlendirme. In A. Karadağ (Ed.), *Kamusal Alan ve Türkiye* (pp. 42–74). Ankara: Asil Yayınları.
- Karagiannopoulos, V. (2018). *Living with hacktivism, from conflict to symbiosis*. Cham: Palgrave Macmillan. doi:10.1007/978-3-319-71758-6
- Karlov, A. (2017). Cybersecurity of Internet of Things – Risks and Opportunities. *Proceedings of the XXVI International Symposium on Nuclear Electronics & Computing*, 182-187.

Compilation of References

- Karn v. United States Dep't of State, 925 F. Supp. 1, 1996 U.S. Dist. LEXIS 5707 (D.D.C., 1996).
- Kash, W. (2014). *Internet Of Things: 8 Cost-Cutting Ideas For Government*. Retrieved 2018, September 23, from <http://www.informationweek.com/government/leadership/internet-of-things-8-cost-cutting-ideas-for-government/d/d-id/1113459>
- Kaspersky Lab. (n.d.). Retrieved from <https://usa.kaspersky.com/resource-center/definitions/social-engineering>
- Kassaye, M., Sherief, H. T., Fissehay, G., & Teklu, T. (1999). Drug use among High School Students in Addis Ababa and Butajira. *EJHD*, 13(2), 101–106.
- Kaster, P., & Sen, P. K. (2014). Power grid cyber security: challenges and impacts. *Proceedings of the 2014 North American Power Symposium (NAPS)*, 1–6. 10.1109/NAPS.2014.6965424
- Katelyn, G., & Holtfreter, K. (2017). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims & Offenders*, 12(5), 741–760. doi:10.1080/15564886.2016.1177766
- Katz, K. L., & Martin, B. R. (1989). Improving customer satisfaction through the management of perceptions of waiting. Massachusetts Institute of Technology. Retrieved from <http://hdl.handle.net/1721.1/37703>
- Kaur, M., & Virk, R. S. (2013). Security System Based on User Authentication Using Keystroke Dynamics||. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(5), 2111–2117.
- Kayode-Adedeji, T., Oyero, O., & Aririguzoh, S. (2017). *Regulating the social media for global relationships*. Paper presented at the 4th International Conference on Education, Social Sciences and Humanities, Dubai, UAE.
- Kc, G. S., Keromytis, A. D., & Prevelakis, V. (2003, October). Countering code-injection attacks with instruction-set randomization. In *Proceedings of the 10th ACM conference on Computer and communications security* (pp. 272–280). ACM.
- Kearney, A. T. (2018). *Cybersecurity in ASEAN: An Urgen Call to Action*. Singapore: Academic Press.
- Keat, T. K., & Mohan, A. (2004). Integration of TAM based electronic commerce models for trust. *The Journal of American Academy of Business, Cambridge*, 5(1/2), 404–410.
- Keefer, A., & Baiget, T. (2001). How it all began: A brief history of the Internet. *Vine*, 31(3), 90–95. doi:10.1108/03055720010804221
- Keenan, J. P. (2000). Blowing the whistle on less serious forms of fraud: A study of executives and managers. *Employee Responsibilities and Rights Journal*, 12(4), 199–217. doi:10.1023/A:1013015926299
- Keith, S., & Martin, M. E. (2005). Cyber-Bullying: Creating a Culture of Respect in a Cyber World. *Reclaiming Children and Youth*, 13(4), 224–228.
- Kejriwal, M., Ding, J., Shao, R., Kumar, A., & Szekely, P. (2017). *FlagIt: A system for minimally supervised human trafficking indicator mining*. arXiv preprint arXiv:1712.03086
- Kejriwal, M., Szekely, P., & Knoblock, C. (2018). Investigative Knowledge Discovery for Combating Illicit Activities. *IEEE Intelligent Systems*, 33(1), 53–63. doi:10.1109/MIS.2018.111144556
- Kelly, E. (2016). Congress looks to boost email privacy; Increase social media surveillance. *USA Today*. Retrieved September 29, 2018 from, <http://www.usatoday.com/story/news/2016/02/21/congress-looks-boost-email-privacy-increase-social-media-surveillance/80557184/>
- Kelly, R. (2017, March 3). Almost 90% of cyber attacks are caused by human error or behaviour. *Chief Executive*. Retrieved from <https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/>

- Kelly, M. (2000). Inequality and crime. *The Review of Economics and Statistics*, 82(4), 530–539. doi:10.1162/003465300559028
- Kennell, R., & Jamieson, L. H. (2003, August). Establishing the Genuinity of Remote Computer Systems. In *USENIX Security Symposium* (pp. 295-308). USENIX.
- Kennell, R., & Jamieson, L. H. (2004). An analysis of proposed attacks against genuinity tests. CERIAS, Purdue Univ.
- Kerbrat-Orecchioni, C. (1986). ‘Nouvelle communication’ et ‘analyse conversationnelle’. *Langue française*, 70, 7-25.
- Kerbrat-Orecchioni, C. (2005). *Le discours en interaction*. Paris: Colin.
- Kernighan, B. W. (2017). *Understanding the digital world: What you need to know about computers, the internet, privacy, and security*. Princeton, NJ: Princeton University Press.
- Khader, M. (2011). Behavioural sciences in Home Team operations: ‘Mindware’ to complement our hardware. *Home Team Journal*, 3, 4–9.
- Khader, M., Neo, L. S., Tan, J., Cheong, D. D., & Chin, J. (2019). Learning from violent extremist attacks: An introduction. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 33–62). Singapore: World Scientific Press.
- Khalique, A, Singh, K., & Sood, S. (2010). Implementation of Elliptic Curve Digital Signature Algorithm. *International Journal of Computer Applications*, 2.
- Khan, E. A. (2018). The Prevention of Electronic Crimes Act 2016: An analysis. *LUMS Law Journal*, 5. Retrieved from <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis>
- Khan, R. (2016, April 13). Controversial cyber crime bill approved by NA. *Dawn*. Retrieved from <https://www.dawn.com/news/1251853>
- Khande, R., & Patil, Y. (2014). Online banking in India: Attacks and preventive measures to minimize risk. *International Conference on Information Communication and Embedded Systems (ICICES2014)*. 10.1109/ICICES.2014.7033940
- Khan, M. S., Ferens, K., & Kinsner, W. (2014). A Chaotic Complexity Measure for Cognitive Machine Classification of Cyber-Attacks on Computer Networks. *International Journal of Cognitive Informatics and Natural Intelligence*, 8(3), 45–69. doi:10.4018/IJCINI.2014070104
- Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. (2014). A taxonomy of botnet behavior, detection, and defense. *IEEE Communications Surveys and Tutorials*, 16(2), 898–924. doi:10.1109/SURV.2013.091213.00134
- Kheradmand, B. (2013). Enhancing Energy Efficiency in Wireless Sensor Networks via Improving Elliptic Curve Digital Signature Algorithm. *World Applied Sciences Journal*, 21(11), 1616–1620.
- Khrais, L. T. (2015). Highlighting the Vulnerabilities of Online Banking System. *Journal of Internet Banking and Commerce*, 20(3). doi:10.4172/1204-5357.1000120
- Kidlogger. (n.d.). *Kidlogger - website*. Retrieved December 10, 2018, from Kidlogger.net
- Kiernan, P. (2018). *Language, Identity and Cycling in the New Media Age Exploring Interpersonal Semiotics in Multi-modal Media and Online Texts*. London: Palgrave Macmillan UK. doi:10.1057/978-1-137-51951-1
- Kieyzun, A., Guo, P. J., Jayaraman, K., & Ernst, M. D. (2009). Automatic creation of SQL injection and cross-sites cripting attacks. *Proceedings of the 31st International Conference on Software Engineering (ICSE 2009)*, 199–209. 10.1109/ICSE.2009.5070521

Compilation of References

- Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, 30(4), 470–486. doi:10.1177/0894439311422689
- Kiggins, R. D. (2014). US Leadership in Cyberspace: Transnational Cybersecurity and Global Governance. In J. F. Kremer & B. Muller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 161–180). Heidelberg, Germany: Springer Press. doi:10.1007/978-3-642-37481-4_10
- Kijsanayotin, B., Pannarunothai, S., & Speedie, S. M. (2009). Factors influencing health information technology adoption in Thailand's community health centers: Applying the UTAUT model. *International Journal of Medical Informatics*, 78(6), 404–416. doi:10.1016/j.ijmedinf.2008.12.005 PMID:19196548
- Kikwai, B. K. (2017). Elliptic Curve Digital Signatures and Their Application in the Bitcoin Crypto-currency Transactions. *International Journal of Scientific and Research Publications*, 7(11).
- Kim, T. H. (2018, October 26). South Korean war on “fake news” raises concern of censorship. *Associated Press*. Retrieved from <https://www.apnews.com/3d14a9663b114644a36e123a7c7bf9b1>
- Kim, Y., Kim, I., & Park, N. (2014). *Analysis of Cyber Attacks and Security Intelligence* (Vol. 274). Mobile, AL: Ubiquitous, and Intelligent Computing. doi:10.1007/978-3-642-40675-1_73
- King, S. T., & Chen, P. M. (2006). implementing malware with virtual machines. *IEEE Symposium on Security and Privacy (S&P'06)*.
- Kiperberg, M., & Zaidenberg, N. (2013). Efficient Remote Authentication. *Journal of Information Warfare*, 12(3), 49–55.
- Kircaburun, K., Kokkinos, C. M., Demetrovics, Z., Király, O., Griffiths, M. D., & Çolak, T. (2018). Problematic Online Behaviors among Adolescents and Emerging Adults: Associations between Cyberbullying Perpetration, Problematic Social Media Use, and Psychosocial Factors. *International Journal of Mental Health and Addiction*. doi:10.1007/11469-018-9894-8
- Kirch, C. (2014). The Grey Hat Hacker. Reconciling Cyberspace Reality and the law. *N. Ky. L. Rev.*, 41, 383.
- Kirka, D., Bajak, F., & Ortutay, B. (2018, December 5). Documents show Facebook used user data as competitive weapon. *Associated Press*. Retrieved from <https://www.apnews.com/f15fe5b986ba4426b4f3267e8e1322f0>
- Kirwan, G. (2018). The Rise of Cybercrime. In C. F. Alison Attrill-Smith (Ed.), *The Oxford Handbook of Cyberpsychology*. Oxford Handbooks Online. doi:10.1093/oxfordhb/9780198812746.013.32
- Kirwan, G., & Power, A. (2013). *Cybercrime: The Psychology of Online Offenders*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511843846
- Kish, S. (2017, May). Massively multiplayer games a platform for terrorism? *Intelligencer*. Retrieved from <http://phcintelligencer.com/2017/05/15/massive-multiplayer-games-a-platform-for-terrorism-2/>
- Kiss, J. (2013). Tor ‘deep web’ servers go offline as Irish man held over child abuse images. *The Guardian*.
- Kiyavash, N., Koushanfar, F., Coleman, T. P., & Rodrigues, M. (2013). A Timing Channel Spyware for the CSMA/CA Protocol. *IEEE Transactions on Information Forensics and Security*.
- Kleffner, J. K., & Dinniss, H. A. (2013). Keeping The Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, 89, 512–539.
- Klein, D., & Wueller, J. (2017). *Fake News: A Legal Perspective*. Retrieved from <http://www.kleinmoynihan.com/fake-news-a-legal-perspective/>

- Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., ... Sewell, T. (2009, October). seL4: Formal verification of an OS kernel. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles* (pp. 207-220). ACM. 10.1145/1629575.1629596
- Klein, J. (2015). Deterring and dissuading cyberterrorism. *Journal of Strategic Security*, 8(4), 23–38. doi:10.5038/1944-0472.8.4.1460
- Kleitman, S., Law, M. K. H., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. [PubMed]. *PLoS One*, 13(10), e0205089. doi:10.1371/journal.pone.0205089
- Klicksafe.de. (2018). *Cyber-Mobbing – was ist das?* McClelland. (1987). *Human Motivation*. Cambridge University Press.
- Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online Child Sexual Exploitation: Prevalence, Process, and Offender Characteristics. *Trauma, Violence & Abuse*, 15(2), 126–139. doi:10.1177/1524838013511543 PMID:24608540
- Kludt, T. (2018). *Trump no puede bloquear usuarios en Twitter, ordena una jueza federal*. Available at <https://cnnespanol.cnn.com/2018/05/23/trump-no-puede-bloquear-usuarios-en-twitter-ordena-una-jueza-federal/>
- Knight, B. (2016). *Teenage girl admits making up migrant rape claim that outraged Germany*. Retrieved from <https://www.theguardian.com/world/2016/jan/31/teenage-girl-made-up-migrant-claim-that-caused-uproar-in-germany>
- Knight, W. (2017, September 20). Finally, a Driverless Car with Some Common Sense. *MIT Technology Review*.
- Knott, A. (2013). *Bitcoin*. Retrieved from Panarchy Website: <https://www.panarchy.org/knott/bitcoin.html>
- Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209. doi:10.1090/S0025-5718-1987-0866109-5
- Kochenderfer-Ladd, B., & Pelletier, M. (2008). Teachers' views and beliefs about bullying: Influences on classroom management strategies and students' coping with peer victimization. *Journal of School Psychology*, 46(4), 431–453. doi:10.1016/j.jsp.2007.07.005 PMID:19083367
- Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., . . . Yarom, Y. (2018). *Spectre attacks: Exploiting speculative execution*. arXiv preprint arXiv:1801.01203
- Koczkodaj, W. W., Mazurek, M., Strzałka, D., Wolny-Dominiak, A., & Woodbury-Smith, M. (2018). Electronic Health Record Breaches as Social Indicators. *Social Indicators Research*. doi:10.1007/11205-018-1837-z
- Koebler, J. (2015). *Six Ways Law Enforcement Monitors the Dark Web*. Retrieved from https://motherboard.vice.com/en_us/article/jp5a9g/six-ways-law-enforcement-monitors-the-dark-web
- Koen, C. Jr, & Im, J. H. (1997). Software piracy and its legal implications. *Information & Management*, 31(5), 265–272. doi:10.1016/S0378-7206(96)01090-7
- Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. doi:10.1016/j.cose.2015.07.002
- Kolhekar, M., & Jadhav, A. (2011). Implementation of Elliptic Curve Cryptology on Text and Images. *International Journal of Enterprise Computing and Business Systems*, 1(2).
- Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *IEEE Computer*, 50(7), 80–84. doi:10.1109/MC.2017.201

Compilation of References

- Kolini, F., & Janczewski, L. (2017). Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies. PACIS 2017 Proceedings.
- Komiak, S. X., & Benbasat, I. (2004). Understanding customer trust in agent-mediated electronic commerce, web-mediated electronic commerce, and traditional commerce. *Information Technology Management*, 5(1-2), 181–207. doi:10.1023/B:ITEM.0000008081.55563.d4
- Komsomolskaya Pravda. (2018). “Momo” game in What’s App. Retrieved August 2018, from <https://www.kp.ru/daily/26860/3906471/>
- Kontostathis, A. (2009). ChatCoder: Toward the tracking and categorization of Internet predators. *Proc. Text Mining Workshop 2009 held in conjunction with the Ninth SIAM International Conference on Data Mining (SDM 2009)*.
- Kontostathis, A., Edwards, L., Bayzick, J., McGhee, I., Leatherman, A., & Moore, K. (2009). Comparison of rule-based to human analysis of chat logs. In *1st International Workshop on Mining Social Media*. Seville: Bubok.
- Körner, A., Tscharaktschiew, N., Schindler, R., Schulz, K., & Rudolph, U. (2016). The Everyday Moral Judge - Autobiographical Recollections of Moral Emotions. *PLoS One*, 11(12), 1–32. doi:10.1371/journal.pone.0167224 PMID:27977699
- Kosinskia, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States*, 110(15), 5802–5805. doi:10.1073/pnas.1218772110 PMID:23479631
- Kosnik, A. (2016). *Rogue Archives: Digital Cultural Memory and Media Fandom*. MIT Press. doi:10.7551/mitpress/10248.001.0001
- Kovacs, E. (2018, March 08). Cortana Can Expose Enterprises to Attacks, Researchers Warn. *Security Week*. Retrieved from <https://www.securityweek.com/cortana-can-expose-enterprises-attacks-researchers-warn>
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. doi:10.1037/a0035618 PMID:24512111
- Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *The Journal of Adolescent Health*, 41(6), 22–30. doi:10.1016/j.jadohealth.2007.08.017 PMID:18047942
- Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2008). *CyberBullying: Bullying in the digital age*. Malden, MA: Blackwell Publishing.
- Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). John Wiley & Sons Ltd.
- Kowalski, R. M., Limber, S. P., & McCord, A. (2018). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*.
- Kowalski, S. E. (2018). Holding Internet Advertising Providers Accountable for Sex Trafficking: Impediments to Criminal Prosecution and a Proposed Response. *The Boston University Public Interest Law Journal*, 99(1). Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edschol&AN=edschol.hein.journals.bupi27.7&site=eds-live>
- Koyun, A., & Al Janabi, E. (2017). *Social Engineering Attacks. Journal of Multidisciplinary Engineering Science and Technology* (Vol. 4). JMEST.

- Kraemer, H., Stice, E., Kazdin, A., Offord, D., & Kupfer, D. (2001). How do risk factors work together? Mediators, moderators, and independent, overlapping, and proxy risk factors. *The American Journal of Psychiatry*, 158(6), 848–856. doi:10.1176/appi.ajp.158.6.848 PMID:11384888
- Kranz, M. (2016). *Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry*. Hoboken, NJ: Wiley.
- Krapp, P. (2011). *Noise Channels: Glitch and Error in Digital Culture*. Minneapolis, MN: University of Minnesota Press. doi:10.5749/minnesota/9780816676248.001.0001
- Krebs, P., Prochaska, J. O., & Rossi, J. S. (2010). A meta-analysis of computer-tailored interventions for health behavior change. *Preventive Medicine*, 51(3–4), 214–221. doi:10.1016/j.ypmed.2010.06.004 PMID:20558196
- Krishnamurthy, Y., Pham, K., Santos, A., & Freire, J. (2016). Interactive exploration for domain discovery on the web. *Proc. of KDD IDEA*.
- Kristol, D. M. (2001). HTTP Cookies: Standards, Privacy, and Politics. *ACM Transactions on Internet Technology*, 1(2), 151–198. doi:10.1145/502152.502153
- Kristy, K., Aldridge, J., DécaryHéту, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *The role of the 'dark web' in the trade of illicit drugs*. WODC, Ministerie van VeiligheidsJustitie, RB-9925-WODC. Retrieved from https://www.rand.org/pubs/research_briefs/RB9925.html
- Krmicek, V. (2011). Inspecting DNS flow traffic for purposes of botnet detection. *GEANT3 JRA2 T4 Internal Deliverable*, 1-9.
- Kroemer, J., & Sen, E. (2006). *No copy: die welt der digitalen raubkopie* (Vol. 24). Klett-Cotta.
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). *Advanced Social Engineering Attacks*. Elsevier.
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. doi:10.1016/j.jisa.2014.09.005
- Kruegel, C., & Kirda, E. (2005). Protecting users against phishing attacks. *The Computer Journal*.
- Kruithof, K., Aldridge, J., DécaryHéту, D., Sim, M., Dujso, E., & Hoorens, S. (2018). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. WODC, Ministerie van VeiligheidsJustitie.
- Kruse, C. S., Frederick, B., Jacobson, T., & Kyle, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. doi:10.3233/THC-161263 PMID:27689562
- Kshetri, N. (2017). *Cybercrime Firms' Internationalization Strategy and Tactics: An Exploratory Framework*. Academic Press.
- Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*. Retrieved September 6, 2019 from, <https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527>
- Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, 52(12), 141–144. doi:10.1145/1610252.1610288
- Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38(11), 1134–1145. doi:10.1016/j.telpol.2014.10.002
- Kubát, M. (2015). Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value. *Procedia Economics and Finance*, 30(15), 409–416. doi:10.1016/S2212-5671(15)01308-8

Compilation of References

- Kuhn, T. S. (1962). The structure of scientific revolutions. *Journal of the History of the Behavioral Sciences*, 2, 274–276.
- Kumar, S., & Shah, N. (2018). *False Information on Web and Social Media: A Survey*. Retrieved from <https://arxiv.org/abs/1804.08559>
- Kumar, G., Kaur, A., & Sethi, S. (2014). Computer network attacks a study. *International Journal of Computer Science and Mobile Applications*, 2(11), 24–32.
- Kushmerick, N., Weld, D. S., & Doorenbos, R. (1997). *Wrapper induction for information extraction*. Academic Press.
- Kuss, D. J., & Griffiths, M. D. (2011). Online Social Networking and Addiction—A Review of the Psychological Literature. *International Journal of Environmental Research and Public Health*, 8(9), 3528–3552. doi:10.3390/ijerph8093528 PMID:22016701
- Kuss, D. J., & Griffiths, M. D. (2017). Social Networking Sites and Addiction: Ten Lessons Learned. *International Journal of Environmental Research and Public Health*, 14(3), 311. doi:10.3390/ijerph14030311 PMID:28304359
- Kuss, D. J., Griffiths, M. D., Karila, L., & Billieux, J. (2014). Internet addiction: A systematic review of epidemiological research for the last decade. *Current Pharmaceutical Design*, 20(25), 4026–4052. doi:10.2174/13816128113199990617 PMID:24001297
- Kwang, K. (2018, July 20). Singapore health system hit by ‘most serious breach of personal data’ in cyberattack; PM Lee’s data targeted. *Channel NewsAsia*. Retrieved from <https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318>
- Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in Human Behavior*, 29(1), 16–25. doi:10.1016/j.chb.2012.07.014
- Kwon, J., & Johnson, M. E. (2015). *The market effect of healthcare security: Do patients care about data breaches?* Paper presented at the workshop on the economics of information security (WEIS 15). Retrieved from <https://pdfs.semanticscholar.org/f3c4/2d80583f5d87957a9dbd8bf0bdd4db3c279d.pdf>
- Kwon, O., Kim, C., & Kim, G. (2013). Factors affecting the intensity of emotional expressions in mobile communications. *Online Information Review*, 37(1), 114–131. doi:10.1108/14684521311311667
- Lacy, L. (2018, December 3). DuckDuckGo is shedding its black sheep status thanks to its dedication to privacy. *AdWeek*. Retrieved from <https://www.adweek.com/digital/duckduckgo-is-shedding-its-black-sheep-status-thanks-to-its-dedication-to-privacy/>
- Laftman, S. B., Modin, B., & Ostberg, V. (2013). Cyberbullying and subjective health: A large-scale study of students in Stockholm, Sweden. *Children and Youth Services Review*, 35(1), 112–119. doi:10.1016/j.childyouth.2012.10.020
- Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on financial sector. Elsevier.
- Langone, A. (2018, March 30). Here’s how Facebook or any other app could use your phone’s microphone to gather data. *Time*. Retrieved from <http://time.com/money/5219041/how-to-turn-off-phone-microphone-facebook-spying/>
- Langos, C. (2012). Cyberbullying: The Challenge to Define. *Cyberpsychology, Behavior, and Social Networking*, 15(6), 285–289. doi:10.1089/cyber.2011.0588 PMID:22703033
- Lanning, K. (2010). *Child molesters: A behavioral analysis for professionals investigating the sexual exploitation of children*. Alexandria, VA: National Center for Missing & Exploited Children.

- Lanzarote Committee. (2015). *Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Solicitation of children for sexual purposes through information and communication technologies (Grooming)*. Retrieved from: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064de98>
- Lanzarote Committee. (2019). *Opinion of the Lanzarote Committee on child sexually suggestive or explicit images and/or videos generated, shared and received by children*. Retrieved from: <https://rm.coe.int/opinion-of-the-lanzarote-committee-on-child-sexually-suggestive-or-exp/168094e72c>
- Laperdrix, P., Rudametkin, W., & Baudry, B. (2016). Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints. 37th IEEE Symposium on Security and Privacy (S&P 2016).
- Lapin, T. (2018). *The surprising number of men who complain of workplace sexual harassment*. Available at <https://nypost.com/2018/04/09/the-surprising-number-of-men-who-complain-of-workplace-sexual-harassment/>
- Larkin, C., Szabo, S., & Mintu-Wimsatt, A. (2017). Academic integrity of graduate online students in a curriculum and instruction program. *International Research in Higher Education*, 2(4), 1–8. doi:10.5430/irhe.v2n4p1
- Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(9), 1–10.
- Latonero, M. (2011). *Human trafficking online: The role of social networking sites and online classifieds*. University of Southern California. Retrieved from https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf
- Latonero, M., Musto, J., Boyd, Z., Boyle, E., Bissel, A., Gibson, K., & Kim, J. (2012). *The rise of mobile and the diffusion of technology-facilitated trafficking*. University of Southern California, Center on Communication Leadership & Policy.
- Lau, L. B., Singh, M. M., & Samsudin, A. (2015). *Trusted system modules for tackling apt via spear-phishing attack in byod environment* (Thesis). Universiti Sains Malaysia.
- Laurie, B., Langley, A., & Kasper, E. (n.d.). *Certificate Transparency*. IETF. doi:10.17487/RFC6962
- Lawcom.gov.uk. (2018). *Hate Crime | Law Commission*. Available at: <https://www.lawcom.gov.uk/project/hate-crime/>
- Lazuras, L., Barkoukis, V., Ourda, D., & Tsorbatzoudis, H. (2013). A process model of cyberbullying in adolescence. *Computers in Human Behavior*, 29(3), 881–887. doi:10.1016/j.chb.2012.12.015
- Leary, M. G. (2008). Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation. *Virginia Journal of Social Policy & the Law*, 15(1), 1–50.
- Lecher, C. (2017, August 30). Neo-Nazis disguised GoFundMe campaign as a ‘family reunion’ in Charlottesville. *The Verge*. Retrieved from <https://www.theverge.com/2017/8/30/16227142/gofundme-campaigns-charlottesville-unite-the-right>
- Lee, H. (2013). *Trends in Cryptocurrency: Understanding Digital Money*. Academic Press.
- Lee, N. (2013). Cyber Warfare: Weapon of Mass Disruption. In *Counterterrorism and Cybersecurity* (2nd ed.). New York, NY: Springer New York.
- Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. Electricity Information Sharing and Analysis Center (E-ISAC). Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
- Leech, M. (2017, September 21). Data breach statistics 2017: First half results are in. *Gemalto*. Retrieved from <https://blog.gemalto.com/security/2017/09/21/new-breach-level-index-findings-for-first-half-of-2017/>

Compilation of References

- Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445–454. doi:10.1080/01449290600879344
- Lee, L. T. (2003). The USA PATRIOT Act and telecommunications: Privacy under attack. *Rutgers Computer & Technology Law Journal*, 29, 371.
- Lee, S., Bae, M., & Kim, H. (2017). Future of IoT Networks: A Survey. *Applied Sciences*, 7(10), 1–25. doi:10.3390/app7101072
- Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *Journal of Economics & Policy*, 1, 511.
- Legal Information Institute. (2018). *Health Care Fraud: An Overview*. Retrieved from https://www.law.cornell.edu/wex/healthcare_fraud#
- Leithauser, T. (2012). FBI targets 'hacktivist' groups, arrests alleged LulzSec members. Cybersecurity Policy Report.
- Leng, J., & Jiang, P. (2016). A deep learning approach for relationship extraction from interaction context in social manufacturing paradigm. *Knowledge-Based Systems*, 100, 188–199. doi:10.1016/j.knosys.2016.03.008
- Lenhart, A. (2012). *Teens, smartphones & texting*. Pew Research Internet Project. Retrieved from <http://www.pewinternet.org/2012/03/19/teens-smartphones-texting>
- Lenhart, A. (2015). *Teens, Social Media & Technology Overview 2015*. Pew Research Center. Retrieved from <http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/>
- Lennon, M. M., & Folkinshteyn, D. (2017). From Bit Valley to Bitcoin: The NASDAQ Odyssey. *Global Journal of Business Research*, 11(1), 85–103.
- Lenzerini, M. (2002, June). Data integration: A theoretical perspective. In *Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (pp. 233–246). ACM. 10.1145/543613.543644
- Lepore, J. (2018, September 16). The Hacking of America. *New York Times*, p. SR1.
- Lerman, K., Minton, S. N., & Knoblock, C. A. (2003). Wrapper maintenance: A machine learning approach. *Journal of Artificial Intelligence Research*, 18, 149–181. doi:10.1613/jair.1145
- Leukfeldt, R. (2017). The human factor examined: directions for future research. In Research Agenda. The human factor in Cybercrime and Cybersecurity, (pp. 67–75). Eleven International Publishing.
- Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551–555. doi:10.1089/cyber.2014.0008 PMID:25080013
- Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, 4(3), 324–327. doi:10.4103/2249-4863.161306 PMID:26288766
- Leung, L., & Lee, P. S. N. (2012). The influences of information literacy, internet addiction and parenting styles on internet risks. *New Media & Society*, 14(1), 117–136. doi:10.1177/1461444811410406
- Levy, S. (1994, June 12). *Battle of the Clipper Chip*. Retrieved from <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all>
- Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic and International Studies.
- Lewman, A. (2016). TOR and links with cryptomarkets. In *The Internet and drug markets* (pp. 33–39). Publications of the European Union.

- Lexisnexis. (2017). *The 2017 LexisNexis true cost of fraud study*. Retrieved Sept 30, 2018 from <https://risk.lexisnexis.com/insights-resources/research/2017-tcof>
- Li, N., Li, T., & Venkatasubramania, S. (2007). t -Closeness : Privacy Beyond k -Anonymity and ϵ -Diversity. *IEEE 23rd International Conference*, (3), 106–115. 10.1109/ICDE.2007.367856
- Li, Y., Chang, M.-C., & Lyu, S. (2018). *In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking*. eprint arXiv:1806.02877
- Li, Z., Sanghi, M., Chen, Y., Kao, Y. M., & Chavez, B. (2006). Hamsa: Fast signature generation for zero-day polymorphic worms with provable attack resilience. *IEEE Symposium on Security and Privacy*.
- Liakat, M. A., Monaco, J. V., Tappert, C. C., & Qiu, M. (2017). Keystroke Biometric Systems for User Authentication. *Journal of Signal Processing Systems for Signal, Image, and Video Technology*, 86(2-3), 175–190. doi:10.1007/11265-016-1114-9
- Liang, Q., & Xiangsui, W. (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House Arts.
- Li, B., Erdin, E., Gunes, M. H., Bebis, G., & Shipley, T. (2013). An overview of anonymity technology usage. *Computer Communications*, 36(12), 1269–1283. doi:10.1016/j.comcom.2013.04.009
- Libert, T. (2015). Exposing the Invisible Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites. *International Journal of Communication*.
- Libicki, M. (2016). *Cyberspace in peace and war*. Annapolis, MD: Naval Institute Press.
- Liedtke, J. (1996). Toward real microkernels. *Communications of the ACM*, 39(9), 70–77. doi:10.1145/234215.234473
- Lightfoot, S. (2017). *Surveillance and privacy on the deep web*. Doi:10.13140/RG.2.2.21692.74889
- Liles, S., Rogers, M., Dietz, J. E., & Larson, D. (2012). Applying traditional military principles to cyber warfare. In *Cyber Conflict (CYCON), 2012 4th International Conference on*, (pp. 1-12). Academic Press.
- Lim, J. (2013, October 30). Ang Mo Kio Town Council website hacked. *The Straits Times*. Retrieved from <https://www.straitstimes.com/singapore/courts-crime/ang-mo-kio-town-council-website-hacked>
- Lim, C. (2018). *Checking how fact-checkers check*. Research & Politics. doi:10.1177/2053168018786848
- Lim, V. K. G., & Teo, T. S. H. (2009). Mind your E-manners : Impact of cyber incivility on employees ' work attitude and behavior. *Information & Management*, 46(8), 419–425. doi:10.1016/j.im.2009.06.006
- Lindgren, S., & Lundström, R. (2011). Pirate culture and hacktivist mobilization: The cultural and social protocols of #wikiLeaks on twitter. *New Media & Society*, 13(6), 999–1018. doi:10.1177/1461444811414833
- Linebarger, P. M. (1948). *Psychological warfare*. Pickle Partners Publishing.
- Linke, B. (2014). *The Fundamentals of an ECDSA Authentication System*. Tutorial Article, Maxim Integrated.
- LinkedIn. (2018). *Your dream job is closer than you think*. Retrieved from <https://www.linkedin.com>
- Liou, J. C., Logapriyan, M., Lai, T. W., Pareja, D., & Sewell, S. (2016). A study of the internet privacy in private browsing mode. *Proceedings of the 3rd multidisciplinary international social networks conference*, 1-7. 10.1145/2955129.2955153
- Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., . . . Hamburg, M. (2018). *Meltdown*. arXiv preprint arXiv:1801.01207

Compilation of References

- Li, Q. (2007). Bullying in the new playground: Research into cyberbullying and cybervictimization. *Australian Journal of Educational Technology*, 23, 435–454.
- Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, 23(4), 1777–1791. doi:10.1016/j.chb.2005.10.005
- Li, Q. (2008). A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Research*, 50(3), 223–234. doi:10.1080/00131880802309333
- Liu, F., & Lee, H. (2010). Use of social network information to enhance collaborative filtering performance. *Expert Systems with Applications*, 37(7), 4772–4778. doi:10.1016/j.eswa.2009.12.061
- Liu, J., Shen, H., Narman, H., Chung, W., & Lin, Z. (2018). A Survey of Mobile Crowdsensing Techniques: A Critical Component for The Internet of Things. *ACM Transactions on Cyber-Physical Systems*, 2(3), 1–26. doi:10.1145/3185504
- Liu, J., Xiao, Y., Li, S., Liang, W., & Philip Chen, C. L. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys and Tutorials*, 14(4), 981–997. doi:10.1109/SURV.2011.122111.00145
- Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet*, 9(3), 1–28. doi:10.3390/fi9030027
- Liu, Y., Cen, R., Zhang, M., Ma, S., & Ru, L. (2008, April). Identifying web spam with user behavior analysis. In *Proceedings of the 4th international workshop on Adversarial information retrieval on the web* (pp. 9-16). ACM. 10.1145/1451983.1451986
- Liu, Y., Cheng, C., Cao, J., & Jiang, T. (2012). An improved authenticated group key transfer protocol based on secret sharing. *IEEE Transactions on Computers*, 62(11), 2335–2336. doi:10.1109/TC.2012.216
- Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management*, 53(1), 53–63. doi:10.1016/j.im.2015.08.006
- Livadas, C., Walsh, R., Lapsley, D., & Strayer, W. (2006). Using machine learning techniques to identify botnet traffic. *Local Computer Networks, Proceedings of the 31st IEEE Conference on*, 967–974.
- Livingstone, S. (2007). Strategies of parental regulation in the media-rich home. *Computers in Human Behavior*, 23(2), 920–941. doi:10.1016/j.chb.2005.08.002
- Li, X. (2013). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology*, 27, 301.
- Loeber, R., & Dishion, T. J. (1984). Boys who fight at home and school: Family conditions influencing cross-setting consistency. *Journal of Consulting and Clinical Psychology*, 52(5), 759–768. doi:10.1037/0022-006X.52.5.759 PMID:6501661
- Löfström, E., Trotman, T., Furnari, M., & Shephard, K. (2015). Who teaches academic integrity and how do they teach it? *Higher Education*, 69(3), 435–448. doi:10.1007/10734-014-9784-3
- Loke, K. F. (2017, February 28). MINDEF Internet system breached; data stolen from national servicemen, employees. *Channel NewsAsia*. Retrieved from <http://www.channelnewsasia.com/news/singapore/mindef-internet-system-breached-data-stolen-from-national-service-7617146>
- Lombardi, A. (2018). Digital in 2018 report: gli utenti internet nel mondo superano i 4 miliardi. In Italia sono più di 43 milioni. We are social.
- Longe, O. B., & Chiemeke, S. C. (2008). Cyber Crime And Criminality. In *Nigeria: What Roles Are Internet Access Points In Playing?* Academic Press.

- Long, M. L., Alison, L. A., & McManus, M. A. (2013). Child pornography and likelihood of contact abuse: A comparison between contact child sexual offenders and noncontact offenders. *Sexual Abuse*, 25(4), 370–395. doi:10.1177/1079063212464398 PMID:23160257
- Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems*, 75, 46–57. doi:10.1016/j.future.2017.04.045
- Lopez-Nicola's, C., & Molina-Castillo, F.J. (2008). Customer knowledge management and e-commerce: the role of customer perceived risk. *International Journal of Information Management*, 28(2), 102-13.
- Lord, N. (2017, July 27). What is a phishing attack? Defining and identifying different types of phishing attacks. *Digital Guardian*. Retrieved from <https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks>
- Lord, C., & Barnett, F. (Eds.). (1989). *Political Warfare and Psychological Operations: Rethinking the US Approach*. DIANE Publishing.
- Lorenzetti, R. (2003). *Consumidores*. Buenos Aires: Rubinzan Culzoni Editores.
- Loshin, D. (2013). *Big data analytics: from strategic planning to enterprise integration with tools, techniques, NoSQL, and graph*. Elsevier.
- Lotz, Z. (2012). My whole life is a hack: how Geohot owned the iPhone, PS3 and inadvertently rallied hacktivists. *engadget*. Retrieved from <https://www.engadget.com/2012/05/01/new-yorker-profiles-geohot/>
- Louchart, S., Aylett, R., Hall, L., Woods, S. & Paiva, A. (2006). FearNot! developing social immersion in the VICTEC and ECIRCUS projects. *Semantic Scholar*.
- Loukides, G., Gkoulalas-Divanis, A., & Malin, B. (2010). Anonymization of electronic medical records for validating genome-wide association studies. *Proceedings of the National Academy of Sciences of the United States of America*, 107(17), 7898–7903. doi:10.1073/pnas.0911686107 PMID:20385806
- Loukides, G., Gkoulalas-Divanis, A., & Shao, J. (2013). Efficient and flexible anonymization of transaction data. *Knowledge and Information Systems*, 36(1), 153–210. doi:10.1007/10115-012-0544-3
- Luarn, P., & Hsieh, A.-Y. (2014). Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities. *Online Information Review*, 38(7), 881–895. doi:10.1108/OIR-03-2014-0076
- Lucas, K., & Aly, A. (2015). Counter narratives to interrupt online radicalisation. A report on the CNOIR project presented to the Department of Attorney General. Australia: Countering online Violent Extremism Research Program, Curtin University.
- Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. New York: Oxford University Press.
- Lucchi, N. (2011). Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. *ARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, 19(3), 645–678.
- Lu, H. P., Hsu, C. L., & Hsu, H. Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security*, 13(2), 106–120. doi:10.1108/09685220510589299
- Luhman, N. (1995). *Social Systems*. Stanford University Press.

Compilation of References

- Luo, H., Wang, J., Han, X., & Zeng, D. (2015). The impact of filler interface on online users' perceived waiting time. In 2015 12th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1–5). Guangzhou, China: IEEE. 10.1109/ICSSSM.2015.7170198
- Luo, X. S., & Wang, P. (2018). *(Up)skirting the law: An online perspective (HTBSC Research Report 12/2018)*. Singapore: Home Team Behavioural Sciences Centre.
- Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, 13(2), 71–94. doi:10.1080/17440572.2012.674183
- Luttrell, R. (2019). *Social Media: How to engage, share, and connect* (3rd ed.). London, UK: Rowman & Littlefield.
- Lyon, D. (2014). *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*. Big Data & Society. doi:10.1177/2053951714541861
- Lyons, K., & Phillips, T. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>
- Lyons, K., Phillips, T., Walker, S., Henley, J., Farrell, P., & Carpentier, M. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>
- M, S. S. (2017). *Authentication tokens facilitate secure transactions in the banking Sector*. Academic Press.
- MacDonald, E. (2017, January 13). The fake news that sealed the fate of Antony and Cleopatra. *The Conversation*. Retrieved from <http://theconversation.com/the-fake-news-that-sealed-the-fate-of-antony-and-cleopatra-71287>
- MacDonald, R. (2007). Social exclusion, youth transitions and criminal careers: Five critical reflections on “risk”. In A. France & R. Homel (Eds.), *Pathways and Crime Prevention. Theory, Policy and Practice*. Cullompton: Willan Publishing.
- Macdonald, S. (2006). *Propaganda and Information Warfare in the Twenty-First Century: Altered images and deception operations*. Routledge. doi:10.4324/9780203967393
- MacDougall, R. D. (2015). Whistleblowing: Don't Encourage It, Prevent It Comment on “Cultures of Silence and Cultures of Voice: The Role of Whistleblowing in Healthcare Organisations”. *International Journal of Health Policy and Management*, 5(3), 189–191. doi:10.15171/ijhpm.2015.190 PMID:26927590
- Machackova, H., Dedkova, L., & Mezulanikova, K. (2015). Brief report: The bystander effect in cyberbullying incidents. *Journal of Adolescence*, 43, 96–99. doi:10.1016/j.adolescence.2015.05.010 PMID:26070168
- Machackova, H., Dedkova, L., Sevcikova, A., & Cerna, A. (2013). Bystanders' support of cyberbullied schoolmates. *Journal of Community & Applied Social Psychology*, 23(1), 25–36. doi:10.1002/casp.2135
- Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). *L-diversity*. *ACM Transactions on Knowledge Discovery from Data*, 1(1), 3. doi:10.1145/1217299.1217302
- Mackey, T. (2018). Opioids and the Internet: Convergence of technology and policy to address the illicit online sales of opioids. *Health Services Insights*, 11, 1–6. doi:10.1177/1178632918800995 PMID:30245569
- Mackey, T., Kalyanam, J., & Kuzmenzo, E. (2018). Solution to Detect, Classify, and Report Illicit Online Marketing and Sales of Controlled Substances via Twitter: Using Machine Learning and Web Forensics to Combat Digital Opioid Access. *Journal of Medical Internet Research*, 20(4), e10029. <https://www.jmir.org/2018/4/e10029/pdf> doi:10.2196/10029 PubMed
- Macmillandictionary.com. (2018). *misandry (noun) definition and synonyms | Macmillan Dictionary*. Available at: <https://www.macmillandictionary.com/dictionary/british/misandry>

- Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology*, 11(1), 78–97.
- Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital 'demimonde'. *Information Communication and Society*, 19(1), 111–126. doi:10.1080/1369118X.2015.1093531
- Madigan, S., Ly, A., Rash, C. L., Ouytsel, J. V., & Temple, J. R. (2018). Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. *JAMA Pediatrics*, 172(4), 327–335. doi:10.1001/jamapediatrics.2017.5314 PMID:29482215
- Madsen, W., Sobel, D. L., Rotenberg, M., & Banisar, D. (1997). Cryptography and liberty: An international survey of encryption policy. *The John Marshall Journal of Computer & Information Law*, 16, 475.
- Magaudda, P. (2010). Hacking Practices and their relevance for Consumer Studies: The example of the 'jailbreaking' of the iPhone. *Consumers, Commodities, and Consumption*, 12(1), 12–11.
- Maguin, E., & Loeber, R. (1996). Academic performance and delinquency. In *Crime and justice: An annual review of research* (vol. 20, pp. 145-264). Chicago: University of Chicago Press.
- Maitanmi, O., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Cyber Crimes and Cyber Laws in Nigeria. *International Journal of Engineering Science*, 2(4), 19–25.
- Major, M. (2012). *Technology and human trafficking*. University of Idaho. Retrieved from http://www2.cs.uidaho.edu/~oman/CS336/Major_HumanTrafficking.pdf
- Makokoba, W. (2018). *What we know about personal data protection in Zimbabwe*. Retrieved December 12, 2018 from, <https://kalabashmedia.com>
- Makuch, E. (2015, December). 77,000 Steam accounts hacked every month, new security measures deployed. *Gamespot*. Retrieved from <http://www.gamespot.com/articles/77000-steam-accounts-hacked-every-month-new-securi/1100-6433003/>
- Mala, G. (2016). *Cybercrime victimization: a study among women victims in Chennai city (PhD thesis)*. Chennai, India: University of Madras. Retrieved from <http://hdl.handle.net/10603/179462>
- Malaysia Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007.
- Malaysia Penal Code Manap, N. (2015). Alignment of Malaysia and Asean Agreements on Ict Laws: A Review. *Brawijaya Law Journal*, 2(1). <https://doi.org.proxyvlib.mmu.edu.my/10.21776/ub.blj.2015.002.01.01>
- Malecki, C. K., & Elliott, S. N. (1999). Adolescents' ratings of perceived social support and its importance: Validation of the Student Social Support Scale. *Psychology in the Schools*, 36(6), 473–483. doi:10.1002/(SICI)1520-6807(199911)36:6<473::AID-PITS3>3.0.CO;2-0
- Manaa, M. E., & Hussein, R. (2016). Preventing cross site scripting attacks in websites. *Asian Journal of Information Technology*, 15(16), 2797–2804.
- Manikandakumar, M., & Ramanujam, E. (2018). Security and Privacy Challenges in Big Data Environment. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 315-325). IGI Global. doi:10.4018/978-1-5225-4100-4.ch017
- Manly, T. S., Leonard, L. N., & Riemenschneider, C. K. (2014). Academic integrity in the information age: Virtues of respect and responsibility. *Journal of Business Ethics*, 127(3), 579–590. doi:10.1007/10551-014-2060-8

Compilation of References

- Manne, K. (2018). *Living in a man's world: the logic of misogyny*. Available at <https://global.oup.com/academic/product/down-girl-9780190604981?cc=au?lang=en?&lang=en&>
- Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, 2(2), 155–184. doi:10.1080/23738871.2017.1366536
- Maras, M. H. (2017). Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking? *Journal of Internet Law*, 21(5), 17–21. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=bth&AN=125989017&site=eds-live>
- Marcan & Bushing. (2008). Console hacking 2008: Wii fail. *25th Chaos Communication Congr.*
- Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior*, 31(5), 381–410. doi:10.1080/01639620903004903
- Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using Routine Activity Theory. *Criminal Justice Review*, 35(4), 412–437. doi:10.1177/0734016809360331
- Marek, R. (2014). *Understanding YouTube: Über die Faszination eines Mediums*. Berlin: De Gruyter.
- Marett, K., Biros, D., & Knode, M. (2004). Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training. *Lecture Notes in Computer Science*, 3073, 187–200. doi:10.1007/978-3-540-25952-7_14
- Marin, E., Diab, A., & Shakarian, P. (2016, September). Product offerings in malicious hacker markets. In 2016 IEEE conference on intelligence and security informatics (ISI) (pp. 187-189). IEEE. doi:10.1109/ISI.2016.7745465
- Markey & Atlasis. (n.d.). *Using decision tree analysis for intrusion detection: a how-to guide*. SANS Institute.
- Markoff, J. (2007). *Cyber attack on U.S. nuclear arms lab linked to China*. Retrieved from <https://www.nytimes.com/2007/12/09/world/americas/09iht-hack.1.8653712.html>
- Markoff, J., & Kramer, A. (2009). *U.S. and Russia Differ on a Treaty for Cyberspace*. Retrieved from <https://www.nytimes.com/2009/06/28/world/28cyber.html?mtrref=www.google.com.tr>
- Mark, W. (2014). *Tor's most visited hidden sites host child abuse images*. BBC News.
- Marneffe, M., Rafferty, A., & Manning, C. (2008) Finding contradictions in text. *Proceedings of ACL-08: HLT*, 1039-1047.
- Marshall, T. H. (1999). *Sosyoloji Sözlüğü*. Ankara: Bilim ve Sanat Yayınları.
- Marshall, T. H., & Bottomore, T. (2000). *Yurttaşlık ve Toplumsal Sınıflar*. Ankara: Gündoğan Yayınları.
- Marsh, C. (2011). Business executives' perceptions of ethical leadership and its development. *Journal of Business Ethics*, 114(3), 565–582. doi:10.1007/10551-012-1366-7
- Marta & Modrzewski. (n.d.). Darknet and Medical Big Data. Deep Internet as a Space for Illegal Trade in Medical Information. Retrieved from <http://www.atut.ig.pl/files/big-data.pdf#page=49>
- Martens, B., & Teuteberg, F. (2012). Decision-making in cloud computing environments: A cost and risk based approach. *Information Systems Frontiers*, 14(4), 871–893. doi:10.1007/10796-011-9317-x
- Marthews, A., & Tucker, C. E. (2017). *Government surveillance and internet search behavior*. Available at SSRN 2412564

- Martin, J. (2017). *Could The Dark Net Pave The Way Towards A Less Harmful Illicit Drug Trade?* Retrieved from https://www.huffingtonpost.com.au/2017/09/14/could-the-dark-net-pave-the-way-towards-a-less-harmful-illicit-drug-trade_a_23206913/
- Martinez-Rodriguez, J. L., Hogan, A., & Lopez-Arevalo, I. (2018). Information extraction meets the Semantic Web: A survey. *Semantic Web*, (Preprint), 1-81.
- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Clinical Research Ed.)*, *j3179*. doi:10.1136/bmj.j3179 PMID:28684400
- Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer. doi:10.1057/9781137399052
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. doi:10.1007/11747-016-0495-4
- Martin, S. J., Goldstein, N., & Cialdini, R. (2014). *The small big: Small changes that spark big influence*. London, UK: Profile books Ltd.
- Martins, R. P. (2018). 4). Punching Above Their Digital Weight. *International Journal of Cyber Warfare & Terrorism*, *8*(2), 32–46. doi:10.4018/IJCWT.2018040103
- Marwick, A., & Lewis, R. (2017). *Media manipulation and disinformation online*. Data & Society.
- Maslow, A. (1943). A theory of human motivation. *Psychological Review*, *50*(4), 370–396. doi:10.1037/h0054346
- Mason, J. (2002). Sampling and selection in qualitative research. *Qualitative Research*, *120*, 144.
- Mason, K. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, *45*(4), 323–348. doi:10.1002/pits.20301
- Matakos, A., Terzi, E. & Tsaparas, P. (2017). Measuring and Moderating Opinion Polarization in Social Networks. *Data Mining and Knowledge Discovery*, *31*(5), 1480-1505. doi:10.1007/10618-017-0527-9
- Mathew, L. A. (2009). Online Child Safety from Sexual Abuse in India. *Journal of Information Law & Technology*, *1*. Retrieved from: https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/mathew
- Mathews, L. (2017, January 27). What is private browsing and why should you use it? *Forbes*. Retrieved from <https://www.forbes.com/sites/leemathews/2017/01/27/what-is-private-browsing-and-why-should-you-use-it/#74686e4e25b1>
- Mathisen, G. E., Øgaard, T., & Einarsen, S. (2012). Individual and situational antecedents of workplace victimization. *International Journal of Manpower*, *33*(5), 539–555. doi:10.1108/01437721211253182
- Matisek, J. W. (2017). Shades of Gray Deterrence: Issues of Fighting in the Gray Zone. *Journal of Strategic Security*, *10*(3), 2. doi:10.5038/1944-0472.10.3.1589
- Matthews, O. (2015, May 7). Russia's greatest weapon may be its hackers. *Newsweek*. Retrieved from <https://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html>
- Mattrick, D. (2013). *Your feedback matters - Update on Xbox One*. Retrieved from <http://news.xbox.com/2013/06/update>
- Matwyshyn, A. M. (2006). Penetrating the zombie collective: Spam as an international security issue. *SCRIPTed*, *3*, 370–388. doi:10.2966/crip.030406.370
- Maurer, T. (2011). *Cybernornorm Emergence at the United Nations: An analysis of the activities at the UN regarding cybersecurity*. Belfer Center for Science and International Affairs. Cambridge, MA: Harvard Kennedy School.

Compilation of References

- Mayer-Schonberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think*. Boston, MA: Houghton Mifflin Harcourt.
- Mayrhofer, P. (2013). Interdependencies in the discovery and adoption of facebook applications: An empirical investigation. Springer.
- Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. US Army War College Strategic Studies Institute Carlisle.
- Mazumdar, A. (2013). Left-wing extremism and counterinsurgency in India: The 'Andhra model'. *Strategic Analysis*, 37(4), 446–462. doi:10.1080/09700161.2013.802518
- McAfee Labs 2018 Threats Predictions Report. (2017). McAfee.
- McAfee. (2009). *The carbon footprint of email spam report*. Retrieved Sept 25, 2018 from <http://resources.mcafee.com/content/NACarbonFootprintSpam>
- McAlaney, J., Frumkin, L., & Benson, V. (2018). *Psychological and Behavioral Examinations in Cyber Security*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-4053-3
- McCabe, D. L., Treviño, L. K., & Butterfield, K. D. (2001). Cheating in academic institutions: A decade of research. *Ethics & Behavior*, 11(3), 219–232. doi:10.1207/S15327019EB1103_2
- McCarthy, J. A. (2010). Internet sexual activity: A comparison between contact and non-contact child pornography offenders. *Journal of Sexual Aggression*, 16(2), 181–195. doi:10.1080/13552601003760006
- McClurg, S. D. (2003). Social Networks and Political Participation: The Role of Social Interaction in Explaining Political Participation. *Political Research Quarterly*, 56(4), 448–465. doi:10.1177/106591290305600407
- McCormack, S. (2006). *United States joins Council of Europe Convention on Cybercrime*. Retrieved from <http://www.state.gov/r/pa/prs/ps/2006/73353.htm>
- McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008). Shining light in dark places: Understanding the tor network. In *International symposium on privacy enhancing technologies symposium* (pp. 63–76). 10.1007/978-3-540-70630-4_5
- McCullagh, N., & Barreto, P. S. (2005, February). A new two-party identity-based authenticated key agreement. In *Cryptographers' Track at the RSA Conference* (pp. 262–274). Springer. 10.1007/978-3-540-30574-3_18
- McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4, 543–568.
- McDonald, S., & Ahern, K. (2002). Physical and Emotional Effects of Whistle blowing. *Journal of Psychosocial Nursing and Mental Health Services*, 40(1), 14–27. doi:10.3928/0279-3695-20020101-09 PMID:11813350
- McFarlane, L., & Bocij, P. (2003). Towards a typology of cyberstalkers. *First Monday*, 8(9). doi:10.5210/fm.v8i9.1076
- McGhee, I., Bayzick, J., Kontostathis, A., Edwards, L., McBride, A., & Jakubowski, E. (2011). Learning to identify Internet sexual predation. *International Journal of Electronic Commerce*, 15(3), 103–122. doi:10.2753/JEC1086-4415150305
- McGillivray. (2015). *What are the effects of social media on youths?* Retrieved from <https://turbofuture.com/internet/effects-of-social-media-on-our-youth>

- McGoogan, C. (2016, February 2). *Dark web browser Tor is overwhelmingly used for crime, says study*, Retrieved from The Telegraph: <http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/>
- McGuinness, D. (2017). *How a cyber attack transformed Estonia*. Retrieved from <https://www.bbc.com/news/39655415>
- McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Research Report 75. Retrieved December 3, 2018, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
- McGuire. (2012). *Organized Crime in the Digital Age*. London: John Grieve Center for Policing and Security.
- McHugh, B., Wisniewski, P., Rosson, M., & Carroll, J. (2018). When social media traumatizes teens: The roles of online risk exposure, coping, and post-traumatic stress. *Internet Research*, 28(5), 1169–1188. doi:10.1108/IntR-02-2017-0077
- McKenna, K. Y. A., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the internet for personality and social psychology. *Personality and Social Psychology Review*, 4(1), 57–75. doi:10.1207/S15327957PSPR0401_6
- McKeown, S., Buivys, M., & Azzopardi, L. (2016, July). InfoScout: An Interactive, Entity Centric, Person Search Tool. In *Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval* (pp. 1113–1116). ACM. 10.1145/2911451.2911468
- McKew, M. (2018, March 19). What *everyone* needs to know about the Facebook data breach. *Cosmopolitan*. Retrieved from <https://www.cosmopolitan.com/politics/a19484431/molly-mckew-facebook-instagram-youtube-manipulating-your-mind/>
- McKinsey & Company. (2017). *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation*. McKinsey & Company.
- McLanahan, S. (1985). Family structure and the reproduction of poverty. *American Journal of Sociology*, 90(4), 873–901. doi:10.1086/228148
- McLean, A. (2019, March 13). *Australia isn't buying local cyber and the rest of the world might soon follow*. Retrieved from <https://www.zdnet.com/google-amp/article/australia-isnt-buying-local-cyber-and-the-rest-of-the-world-might-soon-follow/>
- McManus, M. A., Almond, L., Cubbon, B., Boulton, L., & Mears, I. (2016). Exploring the online communicative themes of child sex offenders. *Journal of Investigative Psychology and Offender Profiling*, 13(2), 166–179. doi:10.1002/jip.1450
- McParkland, T. (2018, July). GameStop agrees to settle data breach class action. *Delaware Law Weekly*. Retrieved from <https://www.law.com/delawarelawweekly/2018/07/16/gamestop-agrees-to-settle-data-breach-class-action/?slreturn=20181012154716>
- McQuade, C. S., Colt, P. J., & Meyer, B. N. (2009). *Cyber bullying: Protecting kids and adults from online bullies*. Westport, CT: Praeger.
- McShane, M. D., & Williams, F. P. III. (2007). *Youth violence and delinquency: Monsters and Myths* (Vol. 1-3). Westport, CT: Greenwood Publishing Group, Inc.
- McWhertor, M. (2015, April). Valve adds two-factor login authentication to Steam mobile app. *Polygon*. Retrieved from <https://www.polygon.com/2015/4/15/8424587/steam-mobile-app-two-factor-login-steam-guard>
- Meadowcroft, B. (2005). *System failure: why systems fail*. Retrieved November 2, 2018 from <http://www.benmeadowcroft.com/reports/systemfailure>
- Meeuwisse, R. (2017). *Cybersecurity For Beginners*. Cyber Simplicity Ltd.

Compilation of References

- Meier, T. (2018). AI technology helps protect teens from cyberbullying. *IBM blog*.
- Mell, P. M., & Grance, T. (2011). *The NIST definition of cloud computing*. doi:10.6028/NIST.SP.800-145
- Meloy, J. R., Hoffmann, J., Guldemann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30(3), 256–279. doi:10.1002/bsl.999 PMID:22556034
- Meloy, J. R., Roshdi, K., Glaz-Ocik, J., & Hoffmann, J. (2015). Investigating the individual terrorist in Europe. *Journal of Threat Assessment and Management*, 2(3-4), 140–152. doi:10.1037/tam0000036
- Méndez-García, V., Jiménez-Ramírez, P., Meléndez-Ramírez, M. Á., Torres-Martínez, F. M., Llamas-Contreras, R., & González, H. (2014). Comparative analysis of banking malware. *IEEE Central America and Panama Convention (CONCAPAN XXXIV)*, 1-5. 10.1109/CONCAPAN.2014.7000412
- Mendhurwar, S., & Mishra, R. (2018). Emerging synergies between Internet of Things and social technologies. *Journal of Global Information Technology Management*, 21(2), 75–80. doi:10.1080/1097198X.2018.1462918
- Mendling, J. (2018). Blockchains for Business Process Management – Challenges and Opportunities. *ACM Trans. Manag. Inform. Syst.*, 9.
- Merabti, M., Kennedy, M., & Hurst, W. (2011). Critical infrastructure protection: A 21st century challenge. *International Conference on Communications and Information Technology*.
- Mercury News. (2015). *Unusual amount of cheating suspected at Stanford University*. Retrieved from <http://news.yahoo.com/unusual-amount-cheating-suspected-stanford-university-165354810.html>
- Merdian, H. L., Moghaddam, N., Boer, D. P., Wilson, N., Thakker, J., Curtis, C., & Dawson, D. (2018). Fantasy-driven versus contact-driven users of child sexual exploitation material: Offender classification and implications for their risk assessment. *Sexual Abuse*, 30(3), 230–253. doi:10.1177/1079063216641109 PMID:27052851
- Merriam-Webster. (2008). *Sexting*. Retrieved from: <https://www.merriam-webster.com/dictionary/sexting>
- Merton, R. (1938). Social structure and anomie. *American Sociological Review*, 3(5), 672–682. doi:10.2307/2084686
- Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *CyberPsychological Behavior*, 12(4), 387–393. doi:10.1089/cpb.2009.0068 PMID:19630583
- Messner, S. (2018, April). How microtransactions and in-game currencies can be used to launder money. *PCGamer*. Retrieved from <https://www.pcgamer.com/how-microtransactions-and-in-game-currencies-can-be-used-to-launder-money/>
- Mhenni, A., Rosenberger, C., Cherrier, E., & Essoukri Ben Amara, N. (2016). Keystroke Template Update with Adapted Thresholds. *International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Monastir, Tunisia. DOI: 10.1109/ATSIP.2016.7523122
- Michael, A., Boniface, A., & Olumide, A. (2014), 'Mitigating Cybercrime and Online Social Networks Threats in Nigeria: *Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz*, 22–24.
- Microsoft Corporation. (2018). *Personal Digital Assistant - Cortana Home Assistant - Microsoft*. Retrieved from Microsoft - Official Home Page: <https://www.microsoft.com/en-us/cortana>
- Microsoft. (2019). *Windows Internet Explorer*. Retrieved from <https://www.microsoft.com/en-us/download/internet-explorer.aspx>

- Middleton, D., Elliott, I. A., Mandeville-Norden, R., & Beech, A. R. (2006). An investigation into the applicability of the Ward and Siegert Pathways Model of child sexual abuse with Internet offenders. *Psychology, Crime & Law*, 12(6), 589–603. doi:10.1080/10683160600558352
- Migliore, D. (2003). *Bullies torment victims with technology*. Retrieved December 9, 2018, from Azprevention.org
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.
- Milkovich, D. (2018, December 3). *13 Alarming Cyber Security Facts and Stats*. Retrieved May 12, 2019, from <https://www.cybintsolutions.com/cyber-security-facts-stats/>
- Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO'85 Proceedings* (pp. 417–426). Springer.
- Miller, G. (2018). *The Apprentice: Trump, Russia and the Subversion of American Democracy*. New York: Custom House.
- Miller, G. A. (1995). WordNet: A lexical database for English. *Communications of the ACM*, 38(11), 39–41. doi:10.1145/219717.219748
- Miller, N. C., Thompson, N. L., & Franz, D. P. (2009). Proactive strategies to safeguard young adolescents in the cyber-age. *Middle School Journal*, 41(1), 28–34. doi:10.1080/00940771.2009.11461701
- Miller, V. (2013). *Understanding digital culture*. London: Sage.
- Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417–426). Springer.
- Miller, W. B. (1958). Lower class culture as a generating milieu of gang delinquency. *The Journal of Social Issues*, 14(3), 5–19. doi:10.1111/j.1540-4560.1958.tb01413.x
- Millie, A. (2009). *Anti-social behaviour*. Open University Press.
- Milne, G., Rohm, A., & Bahl, S. (2004). 'Consumers' protection of online privacy and identity'. *The Journal of Consumer Affairs*, 38(2), 217–232. doi:10.1111/j.1745-6606.2004.tb00865.x
- Milone, M. G. (2002). Hacktivism: Securing the national infrastructure. *Business Lawyer*, 58(1), 383–413.
- Milone, M. G. (2003). Hacktivism: Securing the national infrastructure. *Knowledge, Technology & Policy*, 16(1), 75–103. doi:10.1007/12130-003-1017-5
- Milton, R., Hay, D., Gray, S., Buyuklieva, B., & Hudson-Smith, A. (2018). Smart IoT and Soft AI. *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*, 1–6. 10.1049/cp.2018.0016
- Mingers, J. (2004). Realizing information systems: Critical realism as an underpinning philosophy for information systems. *Information and Organization*, 14(2), 87–103. doi:10.1016/j.infoandorg.2003.06.001
- Mintel. (2018). *Why Mobile Wallets Are Struggling*. Retrieved from <https://thefinancialbrand.com/73332/future-mobile-wallets-payments-trends/>
- Mishna, F., Cook, C., Saini, M., Wu, M. J., & MacFadden, R. (2011). Interventions to prevent and reduce cyber abuse of youth: A systematic review. *Research on Social Work Practice*, 21(1), 5–14. doi:10.1177/1049731509351988
- Mishunin, D. (2018). *How to perform a smart contract audit?* Retrieved from <https://medium.com/hashex-blog/how-to-perform-your-first-smart-contract-audit-3d6883f44924>

Compilation of References

- Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2013). Understanding the decline in unwanted online sexual solicitations for U.S. youth 2000–2010: Findings from three Youth Internet Safety Surveys. *Child Abuse & Neglect*, 37(12), 1225–1236. doi:10.1016/j.chiabu.2013.07.002 PMID:23938019
- Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007). The relative importance of online victimization in understanding depression, delinquency, and substance use. *Child Maltreatment*, 12(4), 314–324. doi:10.1177/1077559507305996 PMID:17954938
- Mitchell, R. (2013). *Instant Web Scraping with Java*. Packt Publishing Ltd.
- Mitchell, R. (2018). *Web Scraping with Python: Collecting More Data from the Modern Web*. O'Reilly Media, Inc.
- Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception*. Academic Press.
- Mitnick, K. (2005). *The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers*. New York: Wiley.
- Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. John Wiley & Sons, Inc.
- Mitnick, K., & Simon, W. (2002). *The art of deception: controlling the human element of security*. New York: Wiley.
- Mkrttchian, V. (2015). Use Online Multi-Cloud Platform Lab with Intellectual Agents: Avatars for Study of Knowledge Visualization & Probability Theory in Bioinformatics. *International Journal of Knowledge Discovery in Bioinformatics*, 5(1), 11-23. Doi:10.4018/IJKDB.2015010102
- Mkrttchian, V. (2015). Modeling using of Triple H-Avatar Technology in online Multi-Cloud Platform Lab. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (3rd ed.; pp. 4162-4170). Hershey: PA: IGI Global. Doi:10.4018/978-1-4666-5888-2.ch409
- Mkrttchian, V., Kataev, M., Hwang, W., Bedi, S., & Fedotova, A. (2016). Using Plug-Avatars “hhh” Technology Education as Service-Oriented Virtual Learning Environment in Sliding Mode. In *Leadership and Personnel Management: Concepts, Methodologies, Tools, and Applications* (pp. 890-902). Hershey, PA: IGI Global. Doi:10.4018/978-1-4666-9624-2.ch039
- Mkrttchian, V., Kataev, M., Shih, T., Kumar, M., & Fedotova, A. (2014). Avatars “HHH” Technology Education Cloud Platform on Sliding Mode Based Plug- Ontology as a Gateway to Improvement of Feedback Control Online Society. *International Journal of Information Communication Technologies and Human Development*, 6(3), 13-31. Doi:10.4018/ijicthd.2014070102
- Mkrttchian, V. (2011). Use ‘hhh’ technology in transformative models of online education. In G. Kurubacak & T. Vokan Yuzer (Eds.), *Handbook of research on transformative online education and liberation: Models for social equality* (pp. 340–351). Hershey, PA: IGI Global. doi:10.4018/978-1-60960-046-4.ch018
- Mkrttchian, V. (2012). Avatar manager and student reflective conversations as the base for describing meta-communication model. In G. Kurubacak, T. Vokan Yuzer, & U. Demiray (Eds.), *Meta-communication for reflective online conversations: Models for distance education* (pp. 340–351). Hershey, PA: IGI Global. doi:10.4018/978-1-61350-071-2.ch005
- Mkrttchian, V., & Aleshina, E. (2017). *Sliding Mode in Intellectual Control and Communication: Emerging Research and Opportunities*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2292-8
- Mkrttchian, V., & Belyanina, L. (Eds.). (2018). *Handbook of Research on Students’ Research Competence in Modern Educational Contexts*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3485-3

- Mkrttchian, V., Bershadsky, A., Bozhday, A., & Fionova, L. (2015). Model in SM of DEE Based on Service-Oriented Interactions at Dynamic Software Product Lines. In G. Kurubacak & T. Yuzer (Eds.), *Identification, Evaluation, and Perceptions of Distance Education Experts* (pp. 231–248). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8119-4.ch014
- Mkrttchian, V., Bershadsky, A., Bozhday, A., Kataev, M., & Kataev, S. (Eds.). (2016). *Handbook of Research on Estimation and Control Techniques in E-Learning systems*. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-9489-7
- Mkrttchian, V., Gamidullaeva, L. A., & Kanarev, S. (2019). Machine Learning With Avatar-Based Management of Sleptsov Net-Processor Platform to Improve Cyber Security. In M. Khan (Ed.), *Machine Learning and Cognitive Science Applications in Cyber Security* (pp. 139–153). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-8100-0.ch006
- Mkrttchian, V., Gamidullaeva, L. A., Vertakova, Y., & Panasenkov, S. (2019). New Tools for Cyber Security Using Blockchain Technology and Avatar-Based Management Technique. In M. Khan (Ed.), *Machine Learning and Cognitive Science Applications in Cyber Security* (pp. 105–122). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-8100-0.ch004
- Mkrttchian, V., Kataev, M., Hwang, W., Bedi, S., & Fedotova, A. (2014). Using Plug-Avatars “hhh” Technology Education as Service-Oriented Virtual Learning Environment in Sliding Mode. In G. Eby & T. Vokan Yuzer (Eds.), *Emerging Priorities and Trends in Distance Education: Communication, Pedagogy, and Technology*. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-5162-3.ch004
- Mkrttchian, V., Veretekhina, S., Gavrilova, O., Ioffe, A., Markosyan, S., & Chernyshenko, S. V. (2019). The Cross-Cultural Analysis of Australia and Russia: Cultures, Small Businesses, and Crossing the Barriers. In U. Benna (Ed.), *Industrial and Urban Growth Policies at the Sub-National, National, and Global Levels* (pp. 229–249). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7625-9.ch012
- Mnih, V., Kavukcuoglu, K., Silver, D., Graves, A., Antonoglou, I., Wierstra, D., & Riedmiller, M. (2013). *Playing Atari with Deep Reinforcement Learning*. eprint arXiv:1312.5602
- Modell, S., & Asher, D. L. (2013). *Pushback: Countering the Iran Action Network*. Center for a New American Security.
- Modus Operandi Law and Legal Definition. (n.d.). In *US Legal*. Retrieved December 3, 2018, from <https://definitions.uslegal.com/m/modus-operandi/>
- Modus Operandi. (n.d.). In *Dictionary by Merriam-Webster*. Retrieved December 6, 2018, from <https://www.merriam-webster.com/dictionary/modus%20operandi>
- Modus Operandi. (n.d.). In *English Oxford Living Dictionaries*. Retrieved December 6, 2018, from https://en.oxforddictionaries.com/definition/modus_operandi
- Moffitt, T. (2018, June 5). American cybercrime: The riskiest states in 2018. *Webroot: Smarter Cybersecurity*. Retrieved from <https://www.webroot.com/blog/2018/06/05/2018-riskiest-states-for-cybercrime-in-america/>
- Moffitt, T. E. (1990). The neuropsychology of juvenile delinquency: A critical review. In M. Tonry & N. Morris (Eds.), *Crime and Justice* (pp. 99–169). University of Chicago Press. doi:10.1086/449165
- Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366–2375. doi:10.1016/j.chb.2012.07.008
- Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Intelligent rule-based phishing websites classification. *IET Information Security*, 8(3), 153–160. doi:10.1049/iet-ifs.2013.0202
- Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(1), 56–63.

Compilation of References

- Moitra, S. D. (2014). *Cybercrime: Towards an Assessment of its Nature and Impact*. Taylor & Francis.
- Mok, Z. C. (2018, March 28). *Spreading Fake News in Singapore Could Get You Punished with These 6 Crimes*. Retrieved from SingaporeLegalAdvice.com website: <https://singaporelegaladvice.com/spreading-fake-news-singapore-crimes>
- Mokhtar, F. (2018, June 19). Cyber threats in Singapore go up; phishing attacks see biggest jump. *Today*. Retrieved from <https://www.todayonline.com/singapore/cyber-threats-singapore-go-phishing-attacks-see-biggest-jump>
- Mokhtar, B., & Azab, M. (2015). Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal*, 54(4), 1115–1126. doi:10.1016/j.aej.2015.07.011
- Monk, B., Mitchell, J., Frank, R., & Davies, G. (2018). Uncovering Tor: An examination of the network structure. *Security and Communication Networks*, 2018, 1–12. doi:10.1155/2018/4231326
- Montazer, G. A., & Yarmohammadi, S. A. (2013). Identifying the critical indicators for phishing detection in Iranian e-banking system. *The 5th Conference on Information and Knowledge Technology (IKT)*, 107–113. 10.1109/IKT.2013.6620048
- Montgomery, H. (2010). Defining Child Trafficking & Child Prostitution: The Case of Thailand Understanding Human Trafficking and Its Victims. *Seattle Journal for Social Justice*, 9, 775–812.
- Mony, S. (2017, November 11). Cambodian Netizens Face New Risks as Government Tightens Online Controls. VOA. Retrieved from <https://www.voanews.com/a/cambodian-netizens-new-risks-governmentonline-controls/4111483.html>
- Moon, D., Im, H., Kim, I., & Park, J. H. (2015). Dtb-ids: An intrusion detection system based on decision tree using behaviour analysis for preventing apt attacks. *The Journal of Supercomputing*, 1–15. doi:10.1007/1227-015-1604-8
- Mooney, A. L., Knox, D., & Schacht, C. (2009). *Understanding social problems*. Wadsworth: Cengage Learning.
- Moore, D., & Rid, T. (2016). *Cryptopolitik and the Darknet*. Retrieved from Taylor and Francis Online Vol. 58 (2016): <http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>
- Moore, M. (2011, May). Chinese labour camp prisoners forced to play online games. *The Telegraph*. Retrieved from <http://www.telegraph.co.uk/technology/news/8537467/Chinese-labour-camp-prisoners-forced-to-play-online-games.html>
- Moore, A. D. (2017). *Intellectual Property and Information Control: Philosophic Foundations and Contemporary Issues*. Philadelphia, PA: Taylor & Francis Publishers. doi:10.4324/9780203788400
- Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 58(1), 7–38. doi:10.1080/00396338.2016.1142085
- Moore, T., & Clayton, R. (2007, June). An Empirical Analysis of the Current State of Phishing Attack and Defence. WEIS.
- Moqbel, M., & Kock, N. (2018). Unveiling the dark side of social networking sites: Personal and work-related consequences of social networking site addiction. *Information & Management*, 55(1), 109–119. doi:10.1016/j.im.2017.05.001
- Morales, A., Falanga, M., Fierrez, J., Sansone, C., & OrtegaGarcia, J. (2015). Keystroke Dynamics Recognition based on Personal Data: A Comparative Experimental Evaluation Implementing Reproducible Research. *Proc. of the IEEE Seventh Int. Conf. on Biometrics: Theory, Applications and Systems*, 1–6. 10.1109/BTAS.2015.7358772
- Morales, A., Fierrez, J., Tolosana, R., Ortega-Garcia, J., Galbally, J., Gomez-Barrero, M., ... Marcel, S. (2016). Keystroke Biometrics Ongoing Competition. *IEEE Access: Practical Innovations, Open Solutions*, 4, 7736–7746. doi:10.1109/ACCESS.2016.2626718
- Morales, K., Sosa-Fey, J., & Farias, J. (2017). Social Media: Are the benefits worth the risks for business? *International Journal of Business and Public Administration*, 14(1), 87–97.

- Moretti, E. (2005). *Does education reduce participation in criminal activities?* National Bureau of Economic Research (NBER).
- Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, 93, 96–105. Retrieved from https://s3.amazonaws.com/academia.edu.documents/49352349/CUSTOMER_DATA-DESIGNING_FOR_TRANSPARENCY_AND_TRUST-R1505H-PDF-ENG.desbloqueado.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1543964166&Signature=52Ri0jn1cWtDJmP%2Fv21vjvzUPu8%3D&response-content-disposition=inline%3B%20filename%3DCustomer_Data_Designing_for_Transparency.pdf
- Morgan, S. (2017). *2017 Cybercrime Report*. Cybersecurity Ventures. Retrieved from <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>
- Morton, T. (2015). *Hyperobjects: Philosophy and Ecology after the End of the World*. University of Minnesota Press.
- Moten, J., Fitterer, A., Brazier, E., Leonard, J., & Brown, A. (2013). Examining online college cyber cheating methods and prevention measures. *Electronic Journal of E-Learning*, 11(2), 139–146.
- Mounteney, J., Griffiths, P., & Vandam, L. (2016). What is the future for internet drug markets? *Insights*, 21, 127–133.
- Mounteney, J., Oteo, A., & Griffiths, P. (2016). The internet and drug markets: shining a light on these complex and dynamic systems. In *The Internet and drug markets* (pp. 13–17). Publications of the European Union.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186–209. doi:10.1016/j.cose.2016.03.004
- Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, 55, 114–127. doi:10.1016/j.cose.2015.09.001
- Mouttapa, M., Valente, T., Gallagher, P., Rohrbach, L. A., & Unger, J. B. (2004). Social network predictor of bullying and victimization. *Adolescence*, 39, 315–335. PMID:15563041
- MPAA. (2006). *The pyramid of internet piracy*. Retrieved from [http://www.mpaa.org/pyramid of piracy.pdf](http://www.mpaa.org/pyramid%20of%20piracy.pdf)
- MS-ISAC. (2018). *MS-ISAC cyber crime technical desk reference*. Retrieved Oct 17, 2018 from <https://www.cisecurity.org/white-papers/ms-isac-cyber-crime-technical-desk-reference/>
- Mubarak, A., & Quinn, S. (2017). General strain theory of Internet addiction and deviant behaviour in social networking sites (SNS). *Journal of Information, Communication and Ethics in Society*. doi:10.1108/JICES-08-2016-0024
- Muggah, R. (2015). The Threat of Organized Crime on Social Media. *World Economic Forum*. Retrieved from <https://www.weforum.org/agenda/2015/07/social-media-violence/>
- Muhammad, L. Q. (2016). Android Mobile Banking Application Security from Reverse Engineering and Network Sniffing. *International Journal of Computer Science and Information Security*, 14(10), 461.
- Muhonen, T., Jönsson, S., & Bäckström, M. (2017). Consequences of cyberbullying behaviour in working life The mediating roles of social support and social organizational climate. *International Journal of Workplace Health Management*, 10(5), 376–390. doi:10.1108/IJWHM-10-2016-0075 PMID:29721038
- Mullen, P. E., & Pathé, M. P. R. (2000). *Stalkers and their victims*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9781139106863
- Munson, L. (2013). *Tor usage doubles in August. New privacy-seeking users or botnet*. Academic Press.

Compilation of References

- Munzert, S., Rubba, C., Meißner, P., & Nyhuis, D. (2014). *Automated data collection with R: A practical guide to web scraping and text mining*. John Wiley & Sons. doi:10.1002/9781118834732
- Murkhejee, A., Liu, B., & Glance, N. (2013) Spotting fake reviewer groups in consumer reviews. In *Proceedings of the 21st International Conference on the World Wide Web*. ACM.
- Muslea, I., Minton, S., & Knoblock, C. (1998, July). Stalker: Learning extraction rules for semistructured, web-based information sources. In *Proceedings of AAAI-98 Workshop on AI and Information Integration* (pp. 74-81). AAAI Press.
- My Activity. (n.d.). *Google*. Retrieved from <https://myactivity.google.com/myactivity>
- MyCERT Incident Statistics. (2018). Retrieved December 6, 2018 from <https://www.mycert.org.my/statistics/2018.php>
- Myers, D., & McGuffee, J. W. (2015). Choosing scrapy. *Journal of Computing Sciences in Colleges*, 31(1), 83–89.
- nA.: Oberösterreichische Nachrichten. (2018, December 5). *Cyber-Stalker ließ 55-jährige Frau im Internet sterben und meldete sie ab. Oberösterreichische Nachrichten*. Retrieved from <https://www.nachrichten.at/oberoesterreich/steyr/Cyber-Stalker-liess-55-jaehrige-Frau-im-Internet-sterben-und-meldete-sie-ab;art68,3071034>
- Nadeau, M. (2018). *Data breach predictions for 2019*. CSO, IDG Communications, Inc. Retrieved from <https://www.csoononline.com/article/3328396/data-breach/13-data-breach-predictions-for-2019.html>
- Nadi, Y., & Firth, L. (2004). The Internet Implication in Expanding Individual Freedom in Authoritarian States. *ACIS 2004 Proceedings*.
- Nagargoje, Y. R., Lomte, S. S., Auti, R. A., & Rokade, A. H. (2014). Security using Fusion of Keystroke and Mouse Dynamics, *International Journal Of Scientific. Research in Education*, 2(7), 1185–1194.
- Nair, S. K. (n.d.). The ethicality of whistleblowing and its implications for human resource management. *Indian Journal of Industrial Relations*, 38, 96–112.
- Naito, K. (2017). A Survey on the Internet-of-Things: Standards, Challenges and Future Prospects. *Journal of Information Processing*, 25(0), 23–31. doi:10.2197/ipsjjip.25.23
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Academic Press.
- Nakashima, E., & Timberg, C. (2017). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loosethen-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html
- Nam, D., & Kejriwal, M. (2018). How Do Organizations Publish Semantic Markup? Three Case Studies Using Public Schema. org Crawls. *Computer*, 51(6), 42–51. doi:10.1109/MC.2018.2701635
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.
- Narula, S. (2004). Psychological operations (PSYOPs): A conceptual overview. *Strategic Analysis*, 28(1), 177–192. doi:10.1080/09700160408450124
- National Communications Authority. (2017). *Workshop on Cybercrime Statistics Opens in Accra*. Author.
- National Conference of State Legislatures. (2017, March 30). *Safe Harbor: State Efforts to Combat Child Trafficking*. Retrieved from <http://www.ncsl.org/research/civil-and-criminal-justice/safe-harbor-state-efforts-to-combat-child-trafficking.aspx>

- National Conference of State Legislatures. (2018, June 1). *Human Trafficking Overview*. Retrieved from <http://www.ncsl.org/research/civil-and-criminal-justice/human-trafficking.aspx>
- National Crime Agency. (2015, December). *Campaign targets UK's youngest cyber criminals*. Retrieved from <http://www.nationalcrimeagency.gov.uk/news/765-campaign-targets-uk-s-youngest-cyber-criminals>
- National Cyber Security Agency (NASCA) Malaysia. (2018, December 6). Retrieved from <https://www.nacsa.gov.my>
- National Cybersecurity Protection Act of 2014 (NCPA) (2014). Pub. L. No. 113-282, 128 Stat. 3066.
- National Defense Authorization Act (NDDA) for Fiscal Year 2018 (2018). Pub. L. No. 115-191, 132 Stat. 1253.
- National Health and Medical Research Council. (2018). *National Statement on Ethical Conduct in Human Research*. Canberra: NHMRC. Retrieved from <https://nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018#block-views-block-file-attachments-content-block-1>
- National Human Trafficking Resource Center (NHTRC). (2018). *NHTRC California state report*. Retrieved from <https://humantraffickinghotline.org/state/california>
- National Institute of Justice. (2012). *Human trafficking*. Retrieved from <http://www.nij.gov/topics/crime/human-trafficking/pages/welcome.aspx>
- NATO Cooperative Cyber Defence Centre of Excellence. (2015). *Cyber Security Strategy Documents*. Retrieved December 3, 2018 from <https://ccdcoe.org/strategies-policies.html>
- Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, 32(1), 81–94. doi:10.1080/02732173.2012.628560
- Nave, G., Minxha, J., Greenberg, D. M., Kosinski, M., Stillwell, D., & Rentfrow, J. (2018). Musical preferences predict personality: Evidence from active listening and facebook likes. *Psychological Science*, 29(7), 1145–1158; Advance online publication. doi:10.1177/0956797618761659 PMID:29587129
- NC Report. (2011). Retrieved March 11, 2018, from http://us.norton.com/content/en/us/home_homeoffice/html/cyber-crimereport/
- NCMEC. (2018). National center for missing & exploited children. *Cyber Tipline Fact Sheet*. Retrieved from <http://www.missingkids.com/cybertipline/2million>
- Ndiaye, N. (2002). *International Organisation for Migration Statement*. On the occasion of the Special Session of the General Assembly on Children, New York, NY.
- Near, J. P., & Miceli, M. P. (1986). Retaliation against whistle blowers: Predictors and effects. *The Journal of Applied Psychology*, 71(1), 137–145. doi:10.1037/0021-9010.71.1.137
- Near, J. P., & Miceli, M. P. (1996). Whistle-blowing: Myth and reality. *Journal of Management*, 22(3), 507–526. doi:10.1177/014920639602200306
- Nelson, T. H. (1981). *Literary machines: The report on, and of, project xanadu, concerning word processing, electronic publishing, hypertext, thinkertoys, tomorrow's intellectual revolution, and certain other topics including knowledge, education and freedom*. Academic Press.
- Nelson, J., Lin, X., Chen, C., Iglesias, J., & Li, J. J. (2016). *Social engineering for security attacks*. MISNC, SI, DS '16. NJ: Union; doi:10.1145/2955129.2955158

Compilation of References

- Neo, L. S. (2018). *Understanding personality, psychosocial, and protective predictors of online violent extremism*. Paper submitted for PhD qualifying Examination and Conversion. Singapore: Nanyang Technological University.
- Neo, L. S., Dillon, L., & Khader, M. (2017). Identifying individuals at risk of being radicalised via the internet. *Security Journal*, 30(4), 1112–1133. doi:10.1057/41284-016-0080-z
- Neo, L. S., Dillon, L., & Tan, J. (2016). *Violent extremist cyber footprints: A guide to understanding and countering online violent extremism* (Rev. ed). Singapore: Home Team Behavioural Sciences Centre.
- Neo, L. S., Khader, M., & Pang, J. S. (2017). Comparing ISIS foreign fighters versus sympathiser: Insights from their Twitter postings. *Home Team Journal*, 7, 87–106.
- Neo, L. S., Shi, P., Wang, Y., Wang, P., Khader, M., & Ong, G. (2013). *Defining Singapore's "anonymous problem" (HTBSC brief research report S02/2013)*. Singapore: Home Team Behavioural Sciences Centre.
- Nergiz, M. E., & Clifton, C. (2007). Thoughts on k-anonymization. *Data & Knowledge Engineering*, 63(3), 622–645. doi:10.1016/j.datak.2007.03.009
- Net Nanny. (n.d.). *Net Nanny website*. Retrieved December 12, 2018 from <https://www.netnanny.com/>
- Newcombe, A. (2015). Child Sex Trafficking: Legal Overview | Center on Children and the Law. *Child Law Practice Today*, 34(10). Retrieved from https://www.americanbar.org/groups/child_law/resources/child_law_practiceonline/child_law_practice/vol-34/october-2015/child-sex-trafficking--legal-overview.html
- Newman, A. L. (2015). What the “right to be forgotten” means for privacy in a digital age. *Science*, 347(6221), 507–508. doi:10.1126/science.aaa4603 PMID:25635090
- Newness, K., Steinert, J., & Viswesvaran, C. (2012). Effects of personality on social network disclosure: Do emotionally intelligent individuals post inappropriate content? *Psihologijske Teme*, 21(3), 473–486.
- Newsome, J., Karp, B., & Song, D. (2005). Polygraph: Automatically generating signatures for polymorphic worms. *IEEE Symposium on Security and Privacy*. 10.1109/SP.2005.15
- Ng, A. (2016, August 7). IBM's Watson gives proper diagnosis for Japanese leukemia patient after doctors were stumped for months. *New York Daily News*.
- Ng, A. (2018, December 7). Tech's invasion of our privacy made us more paranoid in 2018. *CNET*. Retrieved from <https://www.cnet.com/news/techs-invasion-of-our-privacy-made-us-more-paranoid-in-2018/>
- NG_Digital_banking_fraud.pdf. (n.d.). Retrieved from https://static1.squarespace.com/static/551aff08e4b037a3bf1ac8c0/t/59dc80663e00bed1b42b612a/1507623017887/NG_Digital_banking_fraud.pdf
- Ngafeeson, M. (2010). *Cybercrime classification: a motivational model*. Paper presented at the Southwest Decision, Sciences Institute Conference. Retrieved December 3, 2018, from http://www.swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf
- Ngalo, T., Xiao, H., Christianson, B., & Zhang, Y. (2018). Threat Analysis of Software Agents in Online Banking and Payments. *IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, 716 - 723. 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00125
- Ngugi, M. (2005). *Law on Cyber crime Overdue*. Legal Week, Computer Crime Research Centre. Retrieved, December 10, 2018 from <http://www.crime-research.org/news/22.5.2005/982/>

- Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 427 - 436). IEEE. 10.1109/CVPR.2015.7298640
- Nian, L. P., & Chuen, D. L. K. (2015). Introduction to bitcoin. In *Handbook of Digital Currency* (pp. 5–30). Academic Press. doi:10.1016/B978-0-12-802117-0.00001-1
- Nichols, J. J., Nichols, J. J., & Schwartz, G. M. (Eds.). (2010). *After Collapse*. University of Arizona Press.
- Nichols, S. (2018). *Japanese dark-web drug dealers are so polite, they'll offer 'a refund' if you're not satisfied*. Retrieved from https://www.theregister.co.uk/2018/08/08/insights_asia_dark_web_report/on
- Nichols, S. (2018, June 4). Your phone is listening and it's not paranoia. *Vice*. Retrieved from https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia
- Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, 31(4), 418–436. doi:10.1016/j.cose.2012.02.009
- Nield, D. (2018, September 7). The super-private Tor Browser gets a huge update, but should you switch from Chrome? *Gizmodo*. Retrieved from <https://gizmodo.com/the-super-private-tor-browser-gets-a-huge-update-but-s-1828879886>
- Nielsen, M. B., & Einarsen, S. (2012). Outcomes of exposure to workplace bullying: A meta-analytic review. *Work and Stress*, 26(4), 309–332. doi:10.1080/02678373.2012.734709 PMID:23236220
- Nielsen, M. B., & Einarsen, S. V. (2018). What we know, what we do not know, and what we should and could have known about workplace bullying: An overview of the literature and agenda for future research. *Aggression and Violent Behavior*, 42(July), 71–83. doi:10.1016/j.avb.2018.06.007
- NISER (Nigerian Institute of Social and Economic Research). (2007). Report of baseline study on employment generation in the informal sector of Nigerian economy. African capacity building foundation/international labour organization project on strengthening the labour market information and poverty monitoring system in Africa, Ibadan, Nigeria.
- Nissenbaum, H. (2004). *Privacy as contextual integrity*. *Wash. L. Rev.* doi:10.1109/SP.2006.32
- Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, 7(2), 61–73. doi:10.1007/10676-005-4582-3
- Niu, F., Zhang, C., Ré, C., & Shavlik, J. W. (2012). DeepDive: Web-scale Knowledge-base Construction using Statistical Learning and Inference. *VLDS*, 12, 25–28.
- Nixon, C. L. (2014). *Current perspectives : the impact of cyberbullying on adolescent health*. Academic Press.
- Nixon, C. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, 5, 143–158. doi:10.2147/AHMT.S36456 PMID:25177157
- Njuguna, M. E. (2014). *Adoption of Bitcoin in Kenya, a Case Study of Bitpesa*. Academic Press.
- No Internet access for public officers' work computers by next June. (2016, June 8). *Channel NewsAsia*. Retrieved from <https://www.channelnewsasia.com/news/singapore/no-internet-access-for-public-officers-work-computers-by-next-ju-7961140>
- Noar, S. M., Benac, C. N., & Harris, M. S. (2007). Does Tailoring Matter? Meta-Analytic Review of Tailored Print Health Behavior Change Interventions. *Psychological Bulletin*, 133(4), 673–693. doi:10.1037/0033-2909.133.4.673 PMID:17592961

Compilation of References

- Noble, S. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: New York University Press. doi:10.2307/j.ctt1pwt9w5
- Noblit, G. W., & Pink, W. T. (1995). Mapping the alternative paths of the sociology of education. In W. T. Pink & G. W. Noblit (Eds.), *Continuity and contradiction: The futures of the sociology of education* (pp. 1–32). Academic Press.
- Noether, S., Mackenzie, A., & Research Lab, T. M. (2016). Ring Confidential Transactions. *Ledger, 1*, 1–18. doi:10.5195/LEDGER.2016.34
- Nohe, P. (2018, September 27). *Re-Hashed: 2018 Cybercrime Statistics: A closer look at the Web of Profit*. Retrieved May 12, 2019, from <https://www.thesslstore.com/blog/2018-cybercrime-statistics/>
- Norberg, P. A., Horned, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1), 100–126. doi:10.1111/j.1745-6606.2006.00070.x
- Norbutas, L. (2018). Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. *The International Journal on Drug Policy, 56*, 92–100. doi:10.1016/j.drugpo.2018.03.016 PMID:29621742
- Norden, S. (2013). *How the Internet has Changed the Face of Crime* (Unpublished Master's thesis). Retrieved from <http://fgcu.digital.flvc.org/islandora/object/fgcu%3A21423>
- Norouzi, A. (2017). An Integrated survey in Affiliate Marketing Network. *Press Academia Procedia, 42*, 299–309. doi:10.17261/Pressacademia.2017.604
- Norry, A. (2018). *The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin*. Retrieved from <https://blockonomi.com/history-of-silk-road/>
- Northcutt, S. (2007). *Traffic Analysis*. SANS Technology Institute. Retrieved from <https://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis>
- Norton, J. (2016). *TOR and The Dark Net Learn To Avoid NSA Spying And Become Anonymous Online*. Createspace Independent Publishers. Retrieved November 28, 2018, from http://mirror.thelifeofkenneth.com/lib/electronics_archive/TorAndTheDarkNet-JaredNorton.pdf
- Novikov, I. (2019). Bye-Bye False Positives: Using AI to Improve Detection. BSidesSF.
- Noy, N. F., & McGuinness, D. L. (2001). *Ontology Development 101: A Guide to Creating Your First Ontology*. Retrieved from Stanford University website: http://protege.stanford.edu/publications/ontology_development/ontology101.pdf
- Nunamaker, J. Jr, Chen, M., & Purdin, T. (1990). Systems development in information systems research. *Journal of Management Information Systems, 7*(3), 89–106. doi:10.1080/07421222.1990.11517898
- Nurmia, J., Kaskelab, T., Perälä, J., & Oksanen, A. (2017). Seller's reputation and capacity on the illicit drug markets: 11-month study on the Finnish version of the Silk Road. *Drug and Alcohol Dependence, 178*, 201–207.
- Nwogwugwu, U. C., & Uzoechina, B. I. (2015). Impact of Economic Crimes on Nigeria's Economic Prosperity under A Democratic Framework. *International Journal of Business and Management, 10*(9), 163–184. doi:10.5539/ijbm.v10n9p16
- Nye, J. (2011). *The Future of Power in the 21st Century*. Cambridge.
- O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity College Law Review, 16*, 137–160.
- O'Neil, C. (2016). *Weapons of Math Destruction*. Washington, DC: Crown Books.
- Oade, A. (2009). *Managing Workplace Bullying*. Palgrave MacMillan. doi:10.1057/9780230249165

- OAS. (n.d.). The G8 24/7 Network of Point Contacts. Retrieved from *Organization of American States*.
- Ogbuaja, F. M. (2016). Sociological and technological factors that enhance cybercrime and cyber security in Nigeria. *International Journal of Law and Legal Studies*, 4(5), 207–216.
- O’Gorman. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12), 2021–2040.
- Ogunbure, A., A. (2011). The Tuskegee Syphilis Study: Some Ethical Reflections. *Thought and Practice: A Journal of the Philosophical Association of Kenya*, 3, 75–92.
- Ohlin, J.D. (2018). Election Interference: The Real Harm and The Only Solution. *Social Science Research Network*, 1–26. doi:10.2139/ssrn.3276940
- Ojeka, S. A., Ben-Caleb, E., & Ekpe, E.-O. I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing*, 7(2), 340–346.
- Okafor, E. E., Imhonopi, D., & Urim, U. M. (2011). Utilisation of internet services and its impact on teaching and research outputs in private universities in South-Western Nigeria. *Australian Journal of Emerging Technologies and Society*, 9(2), 135–151.
- Okeshola, F. B., & Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), 98–114.
- Olavsrud, T. (2010). *9 Best Defenses Against Social Engineering Attacks*. Retrieved December 6, 2018, from <https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm>
- Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3), 116–125. doi:10.5897/IJSA2013.0510
- Olenik-Shemesh, D., Heiman, T., & Eden, S. (2012). Cyberbullying victimisation in adolescence: Relationships with loneliness and depressive mood. *Emotional & Behavioural Difficulties*, 17(3–4), 361–374. doi:10.1080/13632752.2012.704227
- Oliver, R., Oaks, I. N., & Hoover, J. H. (1994). Family issues and interventions in bully and victim relationships. *The School Counselor*, 41, 199–202.
- Ollmann, G. (2017). The Phishing Guide: Understanding & Preventing Phishing Attacks. Retrieved from <http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf>
- Olson, L., Daggs, J., Ellevold, B., & Rogers, T. (2007). Entrapping the innocent: Toward a theory of child sexual predators’ luring communication. *Communication Theory*, 17(3), 231–251. doi:10.1111/j.1468-2885.2007.00294.x
- Olweus, D. (1993). *Bullying at school. What we know and what we can do*. Malden, MA: Blackwell Publishing.
- Omodunbi, A., Odiase, O., Olaniyan, M., & Esan, O. (2016). Cybercrimes in Nigeria: Analysis, Detection, and Prevention. *Journal of Engineering Technology*, 1(1), 37–42.
- Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention *FUOYE. Journal of Engineering Technology*, 1(1), 37–42.
- Online hate crime to be treated the same as face-to-face crime in the UK. (2018). Retrieved from <https://techcrunch.com/2017/08/21/online-hate-crime-to-be-treated-the-same-as-face-to-face-crime-in-the-uk/?guccounter=1>
- OpenDNS. (n.d.). *Open DNS Family - website*. Retrieved December 10, 2018, from Opendns.com

Compilation of References

- Operation Broken Silence (OBS). (2012). *The Nashville backpage report: An analysis of the online commercial sex industry and human trafficking in Tennessee*. Retrieved from <http://www.operationbrokensilence.org/wp-content/uploads/2012/01/NashvilleBackpageReport.pdf>
- OPM.gov. (n.d.). Cybersecurity resource center. Cybersecurity incidents. *U.S. Office of Personnel Management*. Retrieved from <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>
- Oremus, W. (2018, April). Are you really the product? The history of a dangerous idea. *Slate*. Retrieved from <https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html>
- Orito, Y., & Murata, K. (2005). Privacy protection in Japan: cultural influence on the universal value. *Electronic Proceedings of Ethicomp*, 5.
- Ormsby, E. (2016). Silk Road: insights from interviews with users and vendors. In *The Internet and drug markets* (pp. 33-39). Publications of the European Union.
- OrtegaA. (2016). *Paranoid Fish*. Retrieved from <https://github.com/aOrtega/pafish>
- Orwell, G. (2017). 1984. Boston, MA: Houghton Mifflin Harcourt.
- Orzeata, M. (2016). Mass Media - An Ally or An Enemy in the Struggle Against Terrorism? *International Journal of Communication Research*, 6(2), 133-42. Retrieved from http://www.ijcr.eu/articole/315_06%20Mihail%20ORZEATA.pdf
- Osanaïye, O., Raymond Choo, K.-K., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, 67, 147–165. doi:10.1016/j.jnca.2016.01.001
- Osatuyi, B., & Turel, O. (2018). Tug of war between social self-regulation and habit: Explaining the experience of momentary social media addiction symptoms. *Computers in Human Behavior*, 85, 95–105. doi:10.1016/j.chb.2018.03.037
- Osborne, C. (2018, September 19). Hackers peddle thousands of air miles on the Dark Web for pocket money. *ZDNet*. Retrieved from <https://www.zdnet.com/article/hackers-peddle-thousands-of-air-miles-on-the-dark-web-for-pocket-money/>
- Osgood, D. W. (2000). Poisson-based regression analysis of aggregate crime rates. *Journal of Quantitative Criminology*, 16(1), 21–43. doi:10.1023/A:1007521427059
- Ottawa Coalition to End Violence Against Women. (2016). *Cyber violence*. Retrieved 12th of November 2018 from <https://techwithoutviolence.ca/cyberviolence>
- Ott, M., & Pozzi, F. (2011). Towards a New Era for Cultural Heritage Education: Discussing the Role of ICT. *Computers in Human Behavior*, 27(4), 1365–1371. doi:10.1016/j.chb.2010.07.031
- Ou-Yang, L. (2013). Newspaper: Article scraping & curation. Python Library. Retrieved.
- Owens, J., & Matthews, J. (2008, March). A study of passwords and methods used in brute-force SSH attacks. *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*.
- PAConsulting. (2018, September 20). Why the ‘dark web’ is becoming a cyber security nightmare for businesses. *PA Opinion*. Retrieved from <https://www.paconsulting.com/insights/why-the-dark-web-is-becoming-a-cyber-security-nightmare-for-businesses/>
- Paganini, P. (2016, May). The lucrative but vulnerable gaming industry is ripe for cyberattacks. *Security Affairs*. Retrieved from <http://securityaffairs.co/wordpress/47376/cyber-crime/gaming-industry.html>

- Pagliery, J. (2014, March 10). The Deep Web you don't know about. *CNNtech*. Retrieved from <https://money.cnn.com/2014/03/10/technology/deep-web/index.html>
- Pak, C. (2017, May). News Company's Link Sharing on Twitter as Informative Advertising and Content Signaling. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 312-315). ACM. 10.1145/3027063.3027124
- Palazzi, P. (2017). Transferencia Internacional de datos personales. Nueva Regulación de la Dirección Nacional de Protección de Datos Personales. La Ley, 81(33).
- Palazzi, P. (2003). *Principios para la protección de datos personales en la nueva ley argentina en Revista Derecho Informático, No. 3*. Santa Fe: Editorial Iuris.
- Palfrey, P. (2005). "Stemming the international tide of spam", *A draft model law*. Research Publication.
- Pan, Y., & Ding, X. (2006). Anomaly based web phishing page detection. *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, 381–392.
- Panasiuk, P., Dabrowski, M., Saeed, K., & Bochenska-Wlostowska, K. (2014). The Comparison of the Keystroke Dynamics Databases. In *13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM)*. Ho Chi Minh City, Vietnam: Springer. 10.1007/978-3-662-45237-0_13
- Pang, J. S. (2016). Understanding Personality and Person-specific Predictors of Cyber-based Insider Threat. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 107–128). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch006
- Panier, L. (2008). Une posture éthique en deçà des valeurs? *Protée*, 36(2), 69–78.
- Pannell, G., & Ashman, H. (2010). Anomaly Detection over User Profiles for Intrusion Detection. In *8th Australian Information Security Management Conference*. Edith Cowan University.
- Panopticklick 3.0. Is your browser safe from tracking? (n.d.). *Electronic Frontier Foundation*. Retrieved From <https://panopticklick.eff.org/>
- Pantel, P., Gamon, M., Kannan, A., Fuxman, A., & Lin, T. (2017). *U.S. Patent No. 9,767,201*. Washington, DC: U.S. Patent and Trademark Office.
- Parekh, G., Delatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2018). Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education*, 61(1), 11–20. doi:10.1109/TE.2017.2715174
- Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, 28(3), 1019–1027. doi:10.1016/j.chb.2012.01.004
- Parliament Correspondent. (2018, April 10). Digital security bill 2018 presented in parliament. *bdnews24.com*. Retrieved from <https://bdnews24.com/bangladesh/2018/04/10/digital-security-bill-2018-presented-in-parliament>
- Parmar, P., Rathod, G. B., Rathod, S., & Parikh, A. (2015). Drug Abuse and Illicit Drug Trafficking Vis-A-Vis Human Life – A Review. *Prensa Medica Argentina*, 101, 1. doi:10.4172/lpma.1000144
- Parra, E. (2018). *The path to cyber stalking laws tied to the First State Delaware Online*. Retrieved 12th of November 2018 from <https://www.delawareonline.com/story/news/local/2015/06/13/path-cyberstalking-laws-tied-first-state/71179794/>
- Parris, L., Varjas, K., Meyers, J., & Cutts, H. (2012). High School Students' Perceptions of Coping With Cyberbullying. *Youth & Society*, 44(2), 284–306. doi:10.1177/0044118X11398881

Compilation of References

- Partner S. P. E. A. K. (2015). *Online child abuse material is not 'child pornography'*. Retrieved from: <http://www.partnerspeak.org.au/articles/online-child-abuse-material-is-not-pornography>
- Pastrana, D. (2009). *Rising unemployment and poverty in the Philippines*. Retrieved from www.wsos.org
- Patchin, J. W. (2017, May 16). *Blue Whale Challenge*. Retrieved from Cyberbullying Research Center: <https://cyberbullying.org/blue-whale-challenge>
- Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148–169. doi:10.1177/1541204006286288
- Patel, A., Daftedar, M., Shalan, M., & El-Kharashi, M. W. (2015, March). Embedded hypervisor xvisor: A comparative analysis. In *Parallel, Distributed and Network-Based Processing (PDP), 2015 23rd Euromicro International Conference on* (pp. 682-691). IEEE. 10.1109/PDP.2015.108
- Pathe, M., & Mullen, P. E. (1997). The impact of stalkers on their victims. *The British Journal of Psychiatry*, 170(JAN), 12–17. doi:10.1192/bjp.170.1.12 PMID:9068768
- Patil, D. R., & Patil, J. B. (2016). Malicious web pages detection using static analysis of URLs. *International Journal of Information Security and Cybercrime*, 5(2), 31–50. doi:10.19107/IJISC.2016.02.06
- Patil, R. A., & Renke, A. L. (2016). Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm. *International Journal of Computers and Applications*, 144(9), 27–33. doi:10.5120/ijca2016910432
- Patterson, D. (2018, February 7). *How artificial intelligence is unleashing a new type of cybercrime*. Retrieved from TechRepublic: <https://www.techrepublic.com/article/how-artificial-intelligence-is-unleashing-a-new-type-of-cybercrime/>
- Paul Cichonski, T. M. (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology.
- Paul, B., & Leroy, M. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, (139), 31.
- Paulheim, H. (2017). Knowledge graph refinement: A survey of approaches and evaluation methods. *Semantic Web*, 8(3), 489–508. doi:10.3233/SW-160218
- Paul, K. (2018). Ancient artifacts vs. digital artifacts: New tools for unmasking the sale of illicit antiquities on the Dark Web. *Arts*, 7(12), 1–19.
- Pavlik, K. (2017). Cybercrime, hacking, and legislation. *Journal of Cybersecurity*, 1(1).
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. doi:10.1080/10864415.2003.11044275
- Paynter, J., & Pearson, M. (1998). An analysis of WWW-based Information Systems. In W. S. Chow (Ed.), *Multimedia Information Systems in Practice* (pp. 53–63). Singapore: Springer.
- Paz, O. (1993). Şiir ve Modernite. In M. Küçük (Ed.), *Modernite versus Postmodernite* (pp. 184–206). Ankara: Vadi Yayınları.
- Pelker, C., Palmer, A., Raia, B., & Agosti, J. (2015). Computer Crimes. *The American Criminal Law Review*, 52(4), 793–850.
- Pellegrino, E. D. (1995). Toward a virtue based normative ethics for the health professions. *Kennedy Institute of Ethics Journal*, 5(3), 253–274. doi:10.1353/ken.0.0044 PMID:10144959
- Pendar, N. (2007). Toward spotting the pedophile. Telling victim from predator in text chats. *International Conference on Semantic Computing (ICSC 2007)*.

- Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, 31, 117.
- Pennington, J., Socher, R., & Manning, C. (2014). Glove: Global vectors for word representation. In *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)* (pp. 1532-1543). 10.3115/v1/D14-1162
- Pennycook, G., Cannon, T. D., & Rand, D. G. (2017). Prior exposure increases perceived accuracy of fake news. *SSRN*. Retrieved from <https://ssrn.com/abstract=2958246>
- Peotta (2011). A Formal Classification of Internet Banking Attacks and Vulnerabilities. *International Journal of Computer Science and Information Technology*, 3(1), 186-197.
- Pepper, C. (2018, September 3). Analysis: Australia's Proposed Cybersecurity Bill & its implications for Privacy. *Dark-WebNews*. Retrieved from <https://darkwebnews.com/cyber-security/au-cybersecurity-bill>
- Perdisci, R., Lee, W., & Feamster, N. (2010). Behavioral clustering of http-based malware and signature generation using malicious network traces. *USENIX Symposium on Networked Systems Design and Implementation*.
- Perez-Rosas, V., Kleinberg, B., Lefevre, A., & Mihalcea, R. (2018). Automatic Detection of Fake News. In *Proceedings of the 27th International Conference on Computational Linguistics*. ACM.
- Perhach, P. (2018, November 7). The mad dash to find a cybersecurity force. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html>
- Perren, S., Dooley, J., Shaw, T., & Cross, D. (2010). Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents. *Child and Adolescent Psychiatry and Mental Health*, 4(1), 1–10. doi:10.1186/1753-2000-4-28 PMID:21092266
- Perrin, A. (2018, September 5). Americans are changing their relationship with Facebook. *Pew Research Center*. Retrieved from <http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>
- Peter, A. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*.
- Peters, C., & Broersma, M. J. (Eds.). (2013). Rethinking journalism: trust and participation in a transformed news landscape. Milton Park: Routledge.
- Petit, J. M. (2004). Rights of the Child: Report submitted by the Special Rapporteur on the sale of children, child prostitution and child pornography. UN Economic and Social Council.
- Pew Research Center. (2013). *Anonymity, Privacy, and Security Online*. Retrieved September, 23 2018, from <http://www.pewinternet.org/>
- Pew Research Center. (2014). *Online harassment*. Retrieved from <http://www.pewinternet.org/2014/10/22/online-harassment/>
- Pew Research. (2015). The Demographics of Social Media Users. *Internet & Technology*. Retrieved from <http://www.pewinternet.org/2015/08/19/the-demographics-of-social-media-users/>
- Pew Research. (2018). Social Media Use in 2018. *Internet & Technology*. Retrieved from <https://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>
- Phartiyal, S., Patnaik, S., & Ingram, D. (2018, June 25). When a text can trigger a lynching: WhatsApp struggles with incendiary messages in India. *Reuters*. Retrieved from <https://www.reuters.com/article/us-facebook-india-whatsapp-fake-news-idUSKBN1JL0OW>

Compilation of References

- Phelps, A., & Watt, A. (2014). I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation*, 11(4), 261–272. doi:10.1016/j.diin.2014.08.001
- Phillips, D. (2004). “*Elements of effective software management*”, *the project managers hand book*. IEEE Computer Society Press. doi:10.1109/9780471677772
- Phinney, A. (2001). *Trafficking of women and children for sexual exploitation in the Americas – an introduction to trafficking in the Americas*. Women, Health and Development Program. Pan-American Health Organization. Retrieved December 2, 2018 from <https://www.oas.org/en/cim/docs/Trafficking-Paper%5BEN%5D.pdf>
- PhishLabs. (2018). 2018 Phishing Trends & Intelligence Report: Hacking the Human. Retrieved from www.phishlabs.com
- PhishMe. (2016). 2016 Phishing Susceptibility and Resiliency Report. Retrieved from www.phishme.com
- Piatek, M., Kohno, T., & Krishnamurthy, A. (2008). Challenges and directions for monitoring p2p file sharing networks - or - why my printer received a dmca takedown notice. Hotsec.
- Piazza, F. (2016). Bitcoin in the dark web: A shadow over banking secrecy and a call for global response. *Southern California Interdisciplinary Law Journal*, 26, 521–546.
- Piirsalu, K.-L., Mäe, D., Vassar, T., & Nani, A. (2012). *Privacy issues of Social Networks*. Retrieved September 10, 2016, from, <http://social-networks-privacy.wikidot.com/>
- Pillai, G. K. (2010). Left-Wing Extremism (LWE) in India. *Journal of Defence Studies*, 4(2), 1–9.
- Pinterest. (2018). *Pinterest helps you find ideas to try*. Retrieved from <https://www.pinterest.ie/>
- Pinto, L., & Gupta, A. (2015). *Supersizing Self-supervision: Learning to Grasp from 50K Tries and 700 Robot Hours*. eprint arXiv:1509.06825
- Piper, D. L. A. (2015). *Whistleblowing – an employer’s guide to local compliance*. London: DLA Piper. Retrieved from <https://www.dlapiper.com/en/us/insights/publications/2015/06/whistleblowing-law-2015>
- Piquero, A. R., Macdonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime. *Journal of Quantitative Criminology*, 21(1), 55–71. doi:10.1007/10940-004-1787-2
- Pishghadam, R., & Abbasnejad, H. (2017). Introducing Emotioncy as an Invisible Force Controlling Causal Decisions: A Case of Attribution Theory. *Polish Psychological Bulletin*, 48(1), 129–140. doi:10.1515/ppb-2017-0016
- Pitney, J. J. Jr. (2001). *The art of political warfare*. University of Oklahoma Press.
- Plaza, P. P. (2015). My Mother, My Pimp: Jurisdictional and Evidentiary Issues in Prosecuting Internet-Facilitated Sex Trafficking. *Philippine Law Journal*, 687(4). Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.philplj89.36&site=eds-live>
- Plotnikov, V., Vertakova, Y., & Leontyev, E. (2016). Evaluation of the effectiveness of the telecommunication company’s cluster management. *Economic Computation and Economic Cybernetics Studies and Research*, 50(4), 109–118.
- Plutoo, Derreck, & Naehrwert. (2017). Console Security – Switch. *34th Chaos Communication Congr.*
- Poborliova, M. (2011). Virtual Child Pornography. *Masaryk University Journal of Law and Technology*, 5(2), 241–253.
- Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., & Markatos, E. P. (2010, October). Using social networks to harvest email addresses. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (pp. 11–20). ACM. 10.1145/1866919.1866922

- Polaris Project. (2017). *California statistics*. Retrieved from <https://humantraffickinghotline.org/state/california>
- Polyakov, A. (2018, February 20). How AI-Driven Systems Can Be Hacked. *Forbes*. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2018/02/20/how-ai-driven-systems-can-be-hacked/#597427979df0>
- Polyakova, A., & Boyer, S. (2018). *The Future of Political Warfare: Russia, the West, and Coming Age of Global Digital Competition*. Brookings Institution. Retrieved from <https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf>
- Ponemon Institute. (2017). 2017 Cost of data breach study. Retrieved from <https://www.ibm.com/security/data-breach>
- Ponemon Institute. (2018). *State of Endpoint Security Risk*. Retrieved September 17, 2018, from <https://www.businesswire.com/news/home/20181016005758/en/Study-Reveals64-Organizations-Experienced-Successful-Endpoint>
- Poobalan, D. (2018, June 15). *The Dark Web: Myths, Mysteries and Misconceptions*. Retrieved November 28, 2018, from <https://go.kaspersky.com/rs/802-IJN-240/images/Dark%20Web%2010172017.pdf?aliId=521973948>
- Popek, G. J., & Goldberg, R. P. (1974). Formal requirements for virtualizable third generation architectures. *Communications of the ACM*, 17(7), 412–421. doi:10.1145/361011.361073
- Popvov, O., Bergman, J., & Valassi, C. (2018, November 15). A Framework for a Forensically Sound Harvesting the Dark Web. *Proceedings of the Central European Cybersecurity Conference*.
- Pornari, C. D., & Wood, J. (2010). Peer and cyber aggression in secondary school students: The role of moral disengagement, hostile attribution bias, and outcome expectancies. *Aggressive Behavior*, 36(2), 81–94. doi:10.1002/ab.20336 PMID:20035548
- Porter, J. (2018, November 27). Google accused of GDPR privacy violations by seven countries. *The Verge*. Retrieved from <https://www.theverge.com/2018/11/27/18114111/google-location-tracking-gdpr-challenge-european-deceptive>
- Porter, K. (2018). Analyzing the DarkNetMarkets subreddit for evolutions of tools and trends using LDA topic modeling. *Digital Investigation*, 26, S87–S97. doi:10.1016/j.diin.2018.04.023
- Pospisil, B., Gusenbauer, M., Huber, E., & Hellwig, O. (2017). Cyber-Sicherheitsstrategien – Umsetzung von Zielen durch Kooperation. *Datenschutz und Datensicherheit*, 628–632.
- Pot, M., Paulussen, T. G., Ruiter, R. A., Eekhout, I., de Melker, H. E., Spoelstra, M. E., & Van Keulen, H. M. (2017). Effectiveness of a Web-Based Tailored Intervention With Virtual Assistants Promoting the Acceptability of HPV Vaccination Among Mothers of Invited Girls: Randomized Controlled Trial. *Journal of Medical Internet Research*, 19(9), e312. doi:10.2196/jmir.7449 PMID:28877862
- Poudel, S. (2016). Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security. *Berkeley Technology Law Journal*, 31(2), 997–1022.
- Pouwelse, J., Garbacki, P., Epema, D., & Sips, H. (2005). The bittorrent p2p file-sharing system: Measurements and analysis. In *International workshop on peer-to-peer systems* (pp. 205–216). Academic Press.
- Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3), 267–296. doi:10.1177/0022427810365903
- Preetha, S. S. (2015, May 16). Digital sexual harassment in digital Bangladesh. *The Daily Star*. Retrieved from <https://www.thedailystar.net/in-focus/digital-sexual-harassment-digital-bangladesh-82480>
- Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and `observational instruments. *International Journal of Human-Computer Studies*, 71(12), 1133–1143. doi:10.1016/j.ijhcs.2013.09.002

Compilation of References

Press Information Bureau. (2018). *LWE affected districts*. New Delhi, India: Author.

Press Trust of India. (2018). *Momo Challenge: ICSE association in West Bengal warns schools about 'game', suggests awareness drives for parents and students*. Retrieved November 2018, from <https://www.firstpost.com/india/terrorists-who-killed-bjp-leader-anil-parihar-in-kishtwar-have-been-identified-claims-jammu-and-kashmir-governor-satya-pal-malik-5504271.html>

Pressman, D. E., & Ivan, C. (2016). Internet use and violent extremism: A cyber-VERA risk assessment protocol. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 402–420). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch019

Privacy Badger. (n.d.). *Electronic Frontier Foundation*. Retrieved from <https://www.eff.org/privacybadger/faq>

Privacy not included. (n.d.). *Mozilla Foundation*. Retrieved from <https://foundation.mozilla.org/en/privacynotincluded/>

Privitera, C., & Campbell, M. A. (2009). Cyberbullying: The New Face of Workplace Bullying? *Cyberpsychology & Behavior*, 12(4), 395–400. doi:10.1089/cpb.2009.0025 PMID:19594381

Project Syria (n.d.). *Project Syria_docubase*. Retrieved on December 10, 2018, from Docubase.mit.edu

Proofpoint. (2017). The Human Factor 2017. Retrieved from <https://www.proofpoint.com/sites/default/files/pfpt-en-uk-human-factor-report-2017.pdf>

Prosecuting Hate Crimes. A Practical Guide | OSCE. (2018). Retrieved from <https://www.osce.org/odihr/prosecutorsguide>

Provoost, S., Lau, H. M., Ruward, J., & Riper, H. (2017). Embodied Conversational Agents in Clinical Psychology: A Scoping Review. *Journal of Medical Internet Research*, 19(5), e151. doi:10.2196/jmir.6553 PMID:28487267

Prusty, S., Levine, B. N., & Liberatore, M. (2011). Forensic investigation of the oneswarm anonymous files sharing system. In *Proceedings of the 18th acm conference on computer and communications security* (pp. 201–214). 10.1145/2046707.2046731

Pulkkis, G., Karlsson, J., Westerlund, M., & Tana, J. (2017). Secure and Reliable Internet of Things Systems for Healthcare. In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 169–176). IEEE. 10.1109/FiCloud.2017.50

PwC. (2017). *Global State of Information Security Survey 2017: Singapore highlights*. Retrieved from <https://www.pwc.com.sg/en/risk-assurance/assets/gsis/global-state-of-information-security-survey-2017-sg.pdf>

Qarar, S. (2018, October 23). Cybercrime reports hit a record high in 2018: FIA. *Dawn*. Retrieved from <https://www.dawn.com/news/1440854>

Qin, T., & Burgoon, J. (2007). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *Proceedings of the IEEE Conference on Intelligence and Security Informatics*, (pp. 152–158). 10.1109/ISI.2007.379548

Qin, Y., Sheng, Q., Falkner, N., Dustdar, S., Wang, H., & Vasilakos, A. (2016). When things matter: A survey on data-centric internet of things. *Journal of Network and Computer Applications*, 64, 137–153. doi:10.1016/j.jnca.2015.12.016

Qiu, J. X., Yoon, H. J., Fearn, P. A., & Tourassi, G. D. (2018). Deep learning for automated extraction of primary sites from cancer pathology reports. *IEEE Journal of Biomedical and Health Informatics*, 22(1), 244–251. doi:10.1109/JBHI.2017.2700722 PMID:28475069

Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computing in Science & Engineering*, 2(6), 98–100. doi:10.5923/j.computer.20120206.03

- Quayle, E. (2011). Child pornography. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 343–368). Devon, UK: Willan Publishing.
- Queensland Crime and Corruption Commission. (2017). *Australia's first criminal prosecution for research fraud - A case study from The University of Queensland*. Brisbane: The State of Queensland Crime and Corruption Commission.
- Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and Limitation of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*, 3(9), 369–387.
- Quercia, D., Kosinski, M., Stillwell, D., & Crowcroft, J. (2011). Our Twitter profiles, Our selves: Predicting personality with Twitter. *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. 10.1109/PASSAT/SocialCom.2011.26
- Quetelet, A. (2013). Of the development of the propensity to crime. In *Criminological perspective* (3rd ed.; pp. 23-39). London: SAGE Publications Ltd.
- Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. (2018). Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police. *Knowledge-Based Systems*, 149, 155–168. doi:10.1016/j.knosys.2018.03.010
- Qustodio. (n.d.). *Qustodio website*. Retrieved December 10, 2018 from Qustodio.com
- QZone. (2018). Retrieved from <https://qzone.qq.com/>
- Raban, D. R. (2009). Self-Presentation and the Value of Information in Q&A Websites. *Journal of the American Society for Information Science and Technology*, 60(12), 2465–2473. doi:10.1002/asi.21188
- Rabbany, R., Bayani, D., & Dubrawski, A. (2018, July). Active search of connections for case building and combating human trafficking. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 2120-2129). ACM. 10.1145/3219819.3220103
- Rabbi, A. R. (2017, September 21). Women biggest victims of rising cyber crimes. *Dhaka Tribune*. Retrieved from <https://www.dhakatribune.com/bangladesh/crime/2017/09/21/women-biggest-victims-rising-cyber-crimes>
- Rabinovitch, E. (2007). Staying protected from “social engineering”. *Communications Magazine, IEEE*, 45(9), 20–21. doi:10.1109/MCOM.2007.4342845
- Racketeer Influenced and Corrupt Organizations 18 U.S.C. § 1961-1968
- Radu, S. (2019, May 15). Europe's Data Protection Rules Need Reforms, Report Says. *US News & World Report*. Retrieved from <https://www.usnews.com/news/best-countries/articles/2019-05-15/europes-data-protection-rules-need-reforms-report-says>
- Radu, R. (2014). Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In J. F. Kremer & B. Muller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 3–20). Heidelberg, Germany: Springer Press. doi:10.1007/978-3-642-37481-4_1
- Rafique, S., Humayun, M., Hamid, B., Abbas, A., Akhtar, M., & Iqbal, K. (2015, June). Web application security vulnerabilities detection approaches: A systematic mapping study. In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2015 16th IEEE/ACIS International Conference on* (pp. 1-6). IEEE. 10.1109/SNPD.2015.7176244

Compilation of References

- Rahayu, N. (2017). Indonesian Migrant Worker Policies and the Vulnerability of Women Migrant Workers to Becoming Trafficking Victims: An Overview of Recent Legislation. *Journal of Southeast Asian Human Rights*, (2), 159. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.jseahr1.14&site=eds-live>
- Rahman, R. U., & Tomar, D. S. (2018). Botnet Threats to E-Commerce Web Applications and Their Detection. In *Improving E-Commerce Web Applications Through Business Intelligence Techniques* (pp. 48-81). IGI Global.
- Rahman, R. U., Sahu, D. R., & Tomar, D. S. (2017). Challenges in Securing ESB Against Web Service Attacks. In *Exploring Enterprise Service Bus in the Service-Oriented Architecture Paradigm* (pp. 74-96). IGI Global. doi:10.4018/978-1-5225-2157-0.ch006
- Rahman, R., Tomar, D. S., & Das, S. (2012, May). Dynamic image based captcha. In *Communication Systems and Network Technologies (CSNT), 2012 International Conference on* (pp. 90-94). IEEE. 10.1109/CSNT.2012.29
- Rahman, R. U., & Tomar, D. S. (2018). Security Attacks on Wireless Networks and Their Detection Techniques. In *Emerging Wireless Communication and Network Technologies* (pp. 241-270). Singapore: Springer. doi:10.1007/978-981-13-0396-8_13
- Rajab, M. A., Zarfoss, J., Monroe, F., & Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 41-52. 10.1145/1177080.1177086
- Rajagopal, K. (2017). *Update for the online era*. Retrieved 12th of November 2018 from <https://www.thehindu.com/opinion/op-ed/update-for-the-online-era/article19729572.ece>
- Ramanathan, T. (2014). Law as a tool to promote healthcare safety. *Clinical Governance*, 19(2), 172-180. doi:10.1108/CGIJ-03-2014-0015 PMID:26855615
- Rambam, S. (2010). *Privacy Is Dead – Get Over It at The Next HOPE, July 16-18, 2010 in New York City*. Retrieved February 8, 2018, from https://www.youtube.com/watch?v=DaYn_PkrfvQ
- Ramdeo, S. (2017). *Exposure to workplace bullying: The moderated-mediation effects of personal and contextual factors on work-related outcomes in Trinidad and Tobago* (Unpublished doctoral dissertation). The University of the West Indies, St Augustine, Trinidad.
- Ramirez, E., Brill, J., Ohlhausen, M. K., Wright, J. D., & McSweeney, T. (2014). Data brokers: A call for transparency and accountability. *Federal Trade Commission*. Retrieved from <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>
- Ranger, S. (2018, August 21). What is the IoT? Everything you need to know about the Internet of Things right now. *ZDNet*. Retrieved from <https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/>
- Ranger, S. (2018, December 4). *ZDNet*. Retrieved from ZDNet: <https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/>
- Ransom, H. H. (1977). Congress and Reform of the C.I.A. *Policy Studies Journal: the Journal of the Policy Studies Organization*, 5(4), 476-480. doi:10.1111/j.1541-0072.1977.tb01153.x
- Rapid Rise of Cyber Criminals. (2016, May 20). *Star Online*. Retrieved December 1, 2018 from <https://www.thestar.com.my/opinion/letters/2016/05/20/rapid-rise-of-cyber-criminals/>
- Rashid, F. Y. (2013, July). Why video game companies are lucrative targets for hackers. *Security Week*. Retrieved from <http://www.securityweek.com/why-video-game-companies-are-lucrative-targets-hackers>

- Rashkovski, D., Naumovski, V., & Naumovski, G. (2015). Cybercrime Tendencies and Legislation in the Republic of Macedonia. *European Journal on Criminal Policy and Research*, 22, 127-151.
- Raskauskas, J., & Stoltz, A. D. (2007). *Involvement in Traditional and Electronic Bullying Among Adolescents*. doi:10.1037/0012-1649.43.3.564
- Rawat, D. B., & Bajracharya, C. (2015). Cyber security for smart grid systems: status, challenges and perspectives. *Proceedings of the Southeast Con 2015*, 1–6. 10.1109/SECON.2015.7132891
- Ray, A., & Kaushik, A. (2017). *State transgression on electronic expression: is it for real?* Information and Computer Security; doi:10.1108/ICS-03-2016-0024
- Raybourn, E. M. (1999). *An intercultural computer-based multi-user simulation supporting participant exploration of identity and power in a text-based networked virtual reality: Domacity(TM)MOO*. ProQuest Information & Learning.
- Raymond, J. G., Hughes, D. M., & Gomez, C. J. (2001). Sex trafficking of women in the United States. *Coalition Against Trafficking in Women*. Retrieved from http://bibliobase.sernais.pt:8008/BiblioNET/upload/PDF3/01913_sex_traff_us.pdf
- Ray, S. (2006). Whistleblowing and Organizational Ethics. *Nursing Ethics*, 13(4), 438–445. doi:10.1191/0969733006ne882oa PMID:16838574
- Razzaq, A., Hur, A., Farooq Ahmad, H., & Masood, M. (2013). Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. *Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, 1–6. 10.1109/ISADS.2013.6513420
- Razzaq, M., Ali Qureshi, M., Gill, S., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*, 8(6), 383–388.
- Recalt, R. (2016). *El gobierno gasta \$160 millones al año en redes sociales*. Available at <http://www.perfil.com/politica/el-gobierno-gasta-160-millones-al-ano-en-redes-sociales.phtml>
- Reddit. (2018). *Reddit: the front page of the internet*. Retrieved from <https://www.reddit.com/>
- RedTeam Security Consulting. (2016). *Full Force Red Team*. Retrieved from <https://www.redteamsecure.com/red-teaming/>
- Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation (Abingdon)*, 26(1–2), 81–99. doi:10.1080/13511610.2013.747650
- Regents of the University of California. (2015). *Working to ensure academic integrity at UCSD*. Retrieved from <https://students.ucsd.edu/academics/academic-integrity/index.html>
- Regoli, R. M., & Hewitt, J. D. (2003). *Delinquency in Society* (5th ed.). New York: McGraw-Hill Companies, Inc.
- Reidenberg, J. R., Breaux, T., Carnor, L. F., & French, B. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, 30(1), 39–88. doi:10.15779/Z384K33
- Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197–223). New York: Springer. doi:10.1007/978-1-4614-4139-7_10
- Reints, R. (2018, October 3). “Active and dangerous” North Korean hacking group is behind theft of \$100 million, security firm warns. *Fortune*. Retrieved from <http://fortune.com/2018/10/03/north-korea-hacking-apt38/>
- Reisch, M. S. (2018) Acknowledging the spies on campus. *Chemical and Engineering News*, 96(27). Retrieved from <https://cen.acs.org/policy/intellectual-property/Acknowledging-spies-campus/96/i27>

Compilation of References

- Renard, T. (2018). EU Cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, 1-19.
- Renault, S., & Ingarao, A. (2018). Crowdfunding, quand les fans rétribuent les créateurs du web: Spécificités et enjeux du 'Modèle du pourboire'. *Revue Française de Gestion*, 273, 179-203.
- Reno v. American Civil Liberties Union, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997).
- Renshaw, C. (2016). Human Trafficking in Southeast Asia: Uncovering the Dynamics of State Commitment and Compliance. *Michigan Journal of International Law*, 37(4), 611. Retrieved from <http://proxyvlib.mmu.edu.my/login?url=https://search.ebscohost.com.proxyvlib.mmu.edu.my/login.aspx?direct=true&db=edb&AN=121106877&site=eds-live>
- Renz, B. (2016). Russia and "Hybrid Warfare". *Contemporary Politics*, 22(3), 283–300. doi:10.1080/13569775.2016.1201316
- Report, M. (2013). *APT1: Exposing One of China's Cyber Espionage Units*. Retrieved November 11, 2018, from <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>
- Resh, A., Kiperberg, M., Leon, R., & Zaidenberg, N. J. (2017). Preventing Execution of Unauthorized Native-Code Software. *International Journal of Digital Content Technology and its Applications*, 11.
- Resilience, Safety, and Security Psychology [RSSP] Branch. (2019). *6 big questions about the 'day after' Christchurch mosque shootings* (HTBSC Research Report 07/2019 [revised]). Singapore: Home Team Behavioural Sciences Centre.
- Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216–238. doi:10.1177/0022427811425539
- Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, 60(10), 1119–1139. doi:10.1177/0306624X15572861 PMID:25733745
- Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(11), 1149–1169. doi:10.1177/0093854811421448
- Rezmik, M. (2013). Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. *Touro Law Review*, 29(2), 455–483.
- Rich, C. (2016) *Privacy Laws in Africa and the Near East*. Bloomberg BNA World Data Protection Report.
- Richard. (2018, February 9). Privacy vs. Anonymity. *DarkWebNews*. Retrieved from <https://darkwebnews.com/anonymity/privacy-vs-anonymity/>
- Richet, J.-L. (2013, June). *Laundering money online: A review of cybercriminals' methods. Tools and resources for anti-corruption knowledge – United Nations Office on Drugs and Crime (UNODC)*. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf>
- Rickman, A. (2017). How China and the US are emboldening whistle-blowers in the fight against corporate corruption. *South China Morning Post*. Retrieved from <https://www.scmp.com/comment/insight-opinion/article/2121681/how-china-and-us-are-emboldening-whistle-blowers-fight>
- Rid, T. (2017). *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*. Select Committee on Intelligence, US Senate, 30.
- Rideout, V. J., Roberts, D. F., & Foehr, U. G. (2005). *Generation M: Media in the lives of 8-18-year-olds: Executive summary*. Menlo Park, CA: Henry J. Kaiser Family Foundation.

- Ridout, T. N., Franz, M. M., & Fowler, E. F. (2015). Sponsorship, Disclosure, and Donors: Limiting the Impact of Outside Group Ads. *Political Research Quarterly*, 68(1), 154–166. doi:10.1177/1065912914563545
- Rid, T., & Hecker, M. (2009). *2.0: Irregular Warfare in the Information Age: Irregular Warfare in the Information Age*. War. ABC-CLIO.
- Riek, M., Abramova, S., & Böhme, R. (2017). *Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior*. Academic Press.
- Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), ty004. doi:10.1093/cybsec/ty004
- Risen, T. (2015). The illusion of online privacy. *The US News & World Report*. Retrieved October, 3 2018, from <http://www.usnews.com/news/articles/2015/08/25/the-illusion-of-online-privacy>
- Risk-Based Security. (2017, January). *Data Breach QuickView 2016*. Retrieved from <https://pages.riskbasedsecurity.com/2016-ye-breach-quickview>
- Riva, G. (2005). Virtual Reality in Psychotherapy [Review]. *Cyberpsychology & Behavior*, 8(3), 220–230. doi:10.1089/cpb.2005.8.220 PMID:15971972
- Rizzo, A., Pair, J., Graap, K., Manson, B., McNeerney, P. J., Wiederhold, B., & Spira, J. (2006). *A Virtual Reality Exposure Therapy Application for Iraq War Military Personnel with Post Traumatic Stress Disorder: From Training to Toy to Treatment*. In *Novel Approaches to the Diagnosis and Treatment of Posttraumatic Stress Disorder* (pp. 235–250). Washington, DC: IOS Press.
- Roberts, D. A., Kleiman-Weiner, M., Frank, J. R., Olson, B. A., Maze, D. Z., Gallant, A. R., . . . DuBois, T. M. (2016). *U.S. Patent No. 9,275,132*. Washington, DC: U.S. Patent and Trademark Office.
- Roberts, S. (2014). Cyber wars: Applying conventional laws of war to cyber warfare and non-state actors. *Northern Kentucky Law Review*, 41(3), 535–572.
- Robinson, Jones, & Janicke. (2015). Cyber warfare: Issues and challenges. *Journal of Computers and Security*, 49, 70-94.
- Robinson, L., Helmus, T., Cohen, R., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2018). *Modern Political Warfare: Current Practices and Possible Responses*. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1772.html
- Robinson, M. (2013). The SCADA Threat Landscape. In *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013* (pp. 30-41). BCS.
- Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, 49, 70–94. doi:10.1016/j.cose.2014.11.007
- Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, 114, 70–87. doi:10.1016/j.jnca.2018.04.010
- Robinson, S. N., Robertson, J. C., & Curtis, M. B. (2012). The effects of contextual and wrongdoing attributes on organizational employees' whistleblowing intentions following fraud. *Journal of Business Ethics*, 106(2), 213–227. doi:10.1007/10551-011-0990-y
- Rodday, N. (2016). Hacking a Professional Drone. RSAConference.
- Rogers, E. M., & Shoemaker, F. F. (1971). *Communication of Innovations; A Cross-Cultural Approach*. Academic Press.

Compilation of References

- Rogers, G., & Ashford, T. (2015). Mitigating higher ed cyber attacks. *Association Supporting Computer Users in Education Conference Proceedings*.
- Rogers, K. M. (2006). Viagra, viruses and virgins: A pan-Atlantic comparative analysis on the vanquishing of spam. *Computer Law & Security Report*, 22(3), 228–240. doi:10.1016/j.clsr.2006.01.006
- Rogerson, S. (1998). *Social Values in the Information Society*. FTI Annual Report 1998, Forum of Information Technology, Milan, Italy. Retrieved January 2018, from <http://dehn.slu.edu/courses/fall06/493/rogerson.pdf>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. doi:10.1080/00223980.1975.9915803 PMID:28136248
- Rogojanu, A., & Badea, L. (2014). The Issue of competing Currencies. Case Study – Bitcoin. *Theoretical and Applied Economics*, 21(1), 103–114.
- Romano, A. (2018, April 18). *A new law intended to curb sex trafficking threatens the future of the internet as we know it. The controversial bill package FOSTA-SESTA has already impacted sites like Reddit, Craigslist, and Google — and that's just the start*. Retrieved December 4, 2018 from <https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom>
- Ronchi, A. M. (2009). *E-Culture*. New York: Springer-Verlag, LLC.
- Roodman, D. (2009). How to do xtabond2: An introduction to difference and system GMM in Stata. *The Stata Journal*, 9(1), 86–136. doi:10.1177/1536867X0900900106
- Roos, C. (2015). *The motivation and factors driving crypto-currency adoption in SME's*. Gordon Institute of Business Science. University of Petoria.
- Rosenberg, R. (1992). *The social impact of computers*. San Diego, CA: Academic Press.
- Rosenfeld, A., Zemel, R., & Tsotsos, J. K. (2018). *The Elephant in the Room*. arXiv:1808.03305 [cs.CV]
- Rosen, L. D. (2007). *Me, Myspace, and I: Parenting the Net Generation*. New York: Palgrave Macmillan.
- Rosenthal, R. A. (2005). Economic and crime. In S. Guarino-Ghezzi & A. Javier Trevino (Eds.), *Understanding crime: A multidisciplinary approach* (pp. 61–90). New Providence, NJ: Matthew Bender & Company, Inc.
- Rosner, G., & Kenneally, K. (2017). *Privacy and the Internet of Things: Emerging Frameworks For Policy And Design*. Center For Long-Term Cybersecurity. Retrieved September 5, 2019, from, https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf
- Rossiter, E. J. (n.d.). Reflections of a whistle-blower. *Nature*, 11(357), 434 - 6.
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393–404. doi:10.5465/amr.1998.926617
- Routray, B. P. (2017). *State of Play: Left-wing Extremism in India in 2017*. Retrieved from <http://mantraya.org/state-of-play-left-wing-extremism-in-india-in-2017/>
- Roy Morgan Research. (2001). *Privacy and the Community, July 2001*. Office of the Federal Privacy Commissioner. Retrieved September, 4 2018, from, <http://www.privacy.gov.au/publications/rcommunity.html>
- Rrushi, J. L. (2012). SCADA Protocol Vulnerabilities. In J. Lopez, R. Setola, & S. D. Wolthusen (Eds.), *Critical Infrastructure Protection* (pp. 150–176). Berlin: Springer-Verlag. doi:10.1007/978-3-642-28920-0_8

- Ruiz, M. (2017). Establishing volunteer US cyber defense units: A holistic approach. In *International Conference on Cyber Conflict (CyCon U.S.)* (pp. 45-58). Washington, DC: IEEE. 10.1109/CYCONUS.2017.8167512
- Rutenberg, J. (2019, May 20). The Dark, Faceless Threat to 20 Discourse Online. *New York Times*, p. B1.
- Rutkowska, J., & Tereshkin, A. (2007). IsGameOver () anyone. Black Hat.
- Rutkowska, J. (2006). *Subverting Vista™ kernel for fun and profit*. Black Hat Briefings.
- Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? *Business Horizons*, 60(5), 667–676. doi:10.1016/j.bushor.2017.05.010
- Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 201552nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 1–6. 10.1145/2744769.2747942
- Saeed, I. A., Campus, J. B., Selamat, M. A., Ali, M., & Abuagoub, M. A. (2013). A Survey on Malware and Malware Detection Systems. *International Journal of Computers and Applications*.
- Safi, M. (2017). Facebook allowed child abuse posts to stay online for more than a year, Indian court hears. *The Guardian*. Retrieved 12th of November 2018 from <https://www.theguardian.com/world/2017/nov/03/facebook-allowed-child-abuse-posts-stay-online-year-indian-court-hears>
- Sahin, M. (2010). Teachers' perceptions of bullying in high schools: A Turkish study. *Social Behavior and Personality*, 38(1), 127–142. doi:10.2224/bp.2010.38.1.127
- Şahin, M. (2012). The relationship between the cyberbullying/cybervictimization and loneliness among adolescents. *Children and Youth Services Review*, 34(4), 834–837. doi:10.1016/j.childyouth.2012.01.010
- Sahoo, J., Mohapatra, S., & Lath, R. (2010). Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues. *2010 Second International Conference on Computer and Network Technology*. 10.1109/ICCNT.2010.49
- Saini, H., Rao, Y. S., & Panda, T. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications*, 202-209.
- Saleiro, P., Teixeira, J., Soares, C., & Oliveira, E. (2016, March). Timemachine: Entity-centric search and visualization of news archives. In *European Conference on Information Retrieval* (pp. 845-848). Springer. 10.1007/978-3-319-30671-1_78
- Salo, J., Mantymäki, M., & Islam, A. (2018). The dark side of social media - and Fifty Shades of Grey introduction to the special issue: The dark side of social media. *Internet Research*, 28(5), 1166–1168. doi:10.1108/IntR-10-2018-442
- Salomon, D. (2010). *Trojan Horse. s Elements of Computer Security*. London: Springer-Verlag London Limited. doi:10.1007/978-0-85729-006-9
- Samarati, P., & Sweeney, L. (1998). *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and cell suppression*. Technical report, SRI International. Retrieved October 13, 2018, from https://epic.org/privacy/reidentification/Samarati_Sweeney_paper.pdf
- Samarati, P., & Sweeney, L. (1998). Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement Through Generalization and Suppresion. *Proceedings of the IEEE Symposium on Research in Security and Privacy*, 384–393. 10.1145/1150402.1150499
- Sampangi, R., & Hawkey, K. (2016). Who Are You? It Depends (On What You Ask Me!): Context-Dependent Dynamic User Authentication. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association.

Compilation of References

- Sanders, B. G., Dowland, P. S., & Furnell, S. (2009). An assessment of people's vulnerabilities in relation to personal and sensitive data. *Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance (HAISA 2009)*.
- Sandwell, B. (2010). On the globalisation of crime: The internet and new criminality. In Y. Jewkes & M. Yar (Eds.), *Handbook of internet crime* (pp. 38–66). Uffculme, UK: Willan Publishing.
- Sanger, D. (2018, June 17). We Can't Stop the Hackers. *New York Times*, p. SR4.
- Sanger, D. E., & Broad, W. (2018, Jan 16). Pentagon suggests countering devastating cyberattacks with nuclear arms. *New York Times*. Retrieved from <https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html>
- Sankhwar, S., & Chaturvedi, A. (2018). Woman harassment in digital space in India. *International Journal of Pure and Applied Mathematics*, 118(20), 595–607.
- Santos, N. (2015). *Deep Web*. Tecnico Lisboa. Retrieved November 28, 2018, from <https://fenix.tecnico.ulisboa.pt/downloadFile/563568428719095/csf-18.pdf>
- Sapouna, M., Wolke, D., Vannini, N., Watson, S., Woods, S., Schneider, W., ... Aylett, R. (2010). Virtual Learning Intervention to Reduce Bullying Victimization in Primary School: A Controlled Trial. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, 51(1), 104–112. doi:10.1111/j.1469-7610.2009.02137.x PMID:19703096
- Sargan, J. D. (1958). The Estimation of Economic Relationships using Instrumental Variables. *Econometrica*, 26(3), 393–415. doi:10.2307/1907619
- Saridakis, G., Benson, V., Ezingard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320–330. doi:10.1016/j.techfore.2015.08.012
- Sarita, R. D. (2015). Academic cheating among students: Pressure of parents and teachers. *International Journal of Applied Research*, 1(10), 793–797.
- Saroiu, S., Gummadi, K. P., & Gribble, S. D. (2003). Measuring and analyzing the characteristics of napster and gnutella hosts. *Multimedia Systems*, 9(2), 170–184. doi:10.1007/00530-003-0088-1
- Satariano, A., & Isaac, M. (2018, December 5). Facebook's emails tell a cutthroat tale. *The New York Times*, p. B1.
- Satariano, A., & Perlroth, N. (2019, April 21). Cyberattacks Reveal and Insurance Gray Area. *New York Times*, p. BU1.
- Satitkit, S. (2001). User Perceptions of Web site Design in the Travel Industry: an Evaluation Model (Unpublished MCom project). University of Auckland.
- Savage, C. (2013, February 28). Soldiers admits providing files to Wikileaks. *The New York Times*. Retrieved from <https://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html>
- Sayer, A. (1992). *Method in social science* (2nd ed.). Routledge.
- Şaylan, G. (1999). *Postmodernizm*. Ankara: İmge Yayınevi.
- Sbai, H., Goldsmith, M., Meftali, S., & Happa, J. (2018). A Survey of Keylogger and Screenlogger Attacks in the Banking Sector and Countermeasures to Them. In A. Castiglione, F. Pop, M. Ficco, & F. Palmieri (Eds.), *Lecture Notes in Computer Science: Vol. 11161. Cyberspace Safety and Security. CSS 2018*. Cham: Springer. doi:10.1007/978-3-030-01689-0_2

- Scarfone, K., & Mell, P. (2010). *The common configuration scoring system (ccss): Metrics for software security configuration vulnerabilities*. NIST interagency report, 7502.
- Schaefer, B. P. (2014). Social networks and crime: Applying criminological theories. In C. D. Marcum & G. E. Higgins (Eds.), *Social Networking as a Criminal Enterprise*. Boca Raton, FL: CRC Press. doi:10.1201/b16912-5
- Schaefer, L., & Mazerolle, L. (2017). Putting Process into Routine Activity Theory: Variations in the Control of Crime Opportunities. *Security Journal*, 30(1), 266–289. doi:10.1057j.2015.39
- Schäfer, F. (2009). Ludic Philosophy: Subjectivity, choice and virtual death in digital media. *Digital Culture & Education*, 1. Retrieved from http://www.digitalcultureandeducation.com/uncategorized/dce1016_schafer_html
- Schechner, S. (2018, September 30). Facebook faces potential \$1.63 billion fine in Europe over data breach. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906>
- Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, 16(2), 171–182. doi:10.1007/10676-014-9343-8
- Schick, S. (2018, June 13). Poor password practices put corporate cybersecurity at risk. *Security Intelligence*. Retrieved from <https://securityintelligence.com/news/poor-password-practices-put-corporate-cybersecurity-at-risk/>
- Schimmer, L. (2009). Peer profiling and selection in the i2p anonymous network. Petcon 2009.1.
- Schjolberg, S. (2014). *The History of Cybercrime: 1976-2014*. Norderstedt: Herstellung und Verlag.
- Schjolberg, S., & Helie, S. G. (2011). *A Global Treaty on Cybercrime and Cybersecurity*. Oslo: AiTOslo.
- Schleifer, R. (2014). *Psychological Warfare in the Arab-Israeli Conflict*. Springer. doi:10.1057/9781137467034
- Schmitt, M. N. (2017). *Grey Zones in the International Law of Cyberspace*. Academic Press.
- Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. doi:10.1017/CBO9781139169288
- Schmitt, M. N., & Vihul, L. (Eds.). (2017). *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. doi:10.1017/9781316822524
- Schneider, C., & Leest, U. (2018). *Gefahr, Mobbing und Cybermobbing bei Erwachsenen – die allgegenwärtige Gefahr*. Academic Press.
- Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security and Privacy*, 11(4), 3–4. doi:10.1109/MSP.2013.84
- Schreck, C. J. (1999). Criminal victimisation and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*, 16(3), 633–654. doi:10.1080/07418829900094291
- Schuemie, M. J., van der Straaten, P., Krijn, M., & van der Mast, C. A. P. G. (2001). Research on Presence in Virtual Reality: A Survey. *Cyberpsychology & Behavior*, 4(2), 183–201. doi:10.1089/109493101300117884 PMID:11710246
- Schütz, A., & Luckmann, T. (2003). *Strukturen der Lebenswelt*. Konstanz: UVK.
- Schwartz, M. J. (2012, September 28). PNC bank hit by crowdsourced hacktivist attacks. *Informationweek – Online*. Retrieved from <https://search.proquest.com/docview/1081119777/citation/7A5AA98EDDE3463DPQ/2?accountid=8415>
- Schwartz, L. (2015). *Political Warfare Against the Kremlin*. Palgrave Macmillan.

Compilation of References

- Schweinhart, L. J., & Weikart, D. P. (1980). *Young children grow up: The effect of the Perry preschool program on youths through age 15*. Ypsilanti, MI: High/Scope.
- Schwerha, J. IV. (2004). Cybercrime: Legal Standards Governing the Collection of Digital Evidence. *Information Systems Frontiers*, 6(2), 133–151. doi:10.1023/B:ISFI.0000025782.13582.87
- SCO. (2009). *SCO Documents*. Retrieved from Shanghai Corporation Organization: <http://eng.sectesco.org/documents/>
- Scott, A. (2016, April 11). *Interview: Is Ghana Showing the Most Interest in Bitcoin Right Now?* Retrieved from Bitcoin News: <https://news.bitcoin.com/ghana-interested-bitcoin/>
- Scott, S. V., Zachariadis, M., & Barrett, M. (2013). Methodological implications of critical realism for mixed-methods research. *MIS Quarterly: Management Information Systems*, 37(3), 855–879. doi:10.25300/MISQ/2013/37.3.09
- Seale, K., McDonald, J., Glisson, W., Pardue, H., & Jacobs, M. (2018). MedDevRisk: Risk Analysis Methodology for Networked Medical Devices. *Hawaii International Conference on System Sciences 2018 (HICSS-51)*. 10.24251/HICSS.2018.414
- Seals, M., Hammons, J. O., & Mamiseishvili, K. (2014). Teaching assistants' preparation for, attitudes towards, and experiences with academic dishonesty: Lessons learned. *International Journal on Teaching and Learning in Higher Education*, 26(1), 26–36. Retrieved from <http://search.proquest.com.ezproxylocal.library.nova.edu/docview/1651859266?accountid=6579>
- Seböck, W., & Pospisil, B. (2017). The main societal risks an automated future constitutes. *Proceedings of 25th International Scientific Conference on Economic and Social Development - XVII International Social Congress (ISC-2017)*.
- Security engineering: a guide to building dependable distributed systems. (2008). In R. J. Anderson (Ed.), *Security engineering: a guide to building dependable distributed systems*. Indianapolis, IN: Wiley.
- Security Predictions for 2018 Paradigm Shifts*. (2017, December 5). Retrieved from TrendMicro: <https://www.trend-micro.com>
- Segal, L., Ngugi, B., & Mana, J. (2011). Credit Card Fraud: A New Perspective On Tackling An Intransigent Problem. *Fordham Journal of Corporate & Financial Law*, 16(4), 743-781. Retrieved October 20, 2018, <https://ir.lawnet.fordham.edu/jcfl/vol16/iss4/2>
- Select Committee on Deliberate Online Falsehoods. (2018). *Report Of The Select Committee On Deliberate Online Falsehoods – Causes*. Singapore: Consequences And Countermeasures.
- Selwyn, N. (2004). The information aged: A qualitative study of older adults' use of information and communications technology. *Journal of Aging Studies*, 18(4), 369–384. doi:10.1016/j.jaging.2004.06.008
- Semenov, A. (2013). Principles of social media monitoring and analysis software. *Jyväskylä Studies in Computing*, (168).
- Sengupta, S. (2012, March 17). The soul of the new hacktivist. *The New York Times*. Retrieved from <https://www.nytimes.com/2012/03/18/sunday-review/the-soul-of-the-new-hacktivist.html>
- Sengupta, R. P., & Mukherjee, S. (2018). Crime, Deprivation and Social Sustainability—Evidence across States in India. *Indian Journal of Human Development*, 12(3), 1–24. doi:10.1177/0973703018811173
- Seok, S., & DaCosta, B. (2014). Mitigating online threats while promoting scholarship through awareness-raising interventions: A study of young people's technology use, risky online behavior, and literacy of cyber awareness practices. *International Journal of Digital Literacy and Digital Competence*, 5(4), 47–61. doi:10.4018/ijdlc.2014100104

- Seok, S., & DaCosta, B. (2019). The cyber awareness of online video game players: An examination of their online safety practices and exposure to threats. *International Journal of Cyber Research and Education*, 1(1), 69–77. doi:10.4018/IJCRE.2019010108
- Servigne, P., & Chapelle, G. (2017). *L'entraide, l'autre loi de la jungle*. Éditions Les liens qui libèrent.
- Servigne, P., & Stevens, R. (2015). *Comment tout peut s'effondrer, petit manuel de collapsologie à l'usage des générations présentes*. Paris: Seuil.
- Sethi, P., & Sarangi, S. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, 2017, 1–25. doi:10.1155/2017/9324035
- Seto, M. C., Wood, J. M., Babchishin, K. M., & Flynn, S. (2012). Online solicitation offenders are different from child pornography offenders and lower risk contact sexual offenders. *Law and Human Behavior*, 36(4), 320–330. doi:10.1037/h0093925 PMID:22849417
- Sevcikova, A., Machackova, H., Wright, M. F., Dedkova, L., & Cerna, A. (2015). Social support seeking in relation to parental attachment and peer relationships among victims of cyberbullying. *Australian Journal of Guidance & Counseling*, 15, 1–13. doi:10.1017/jgc.2015.1
- Severin, J., & Tankard, J. (1987). *Communication theories: Origins, Methods, Uses*. New York: Hastings House.
- Seymour, J., & Tully, P. (2016). Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter. *Black Hat USA*. Retrieved from <https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf>
- Shackelford, S. (2018, November 5). *What the world's first cyber attack has taught us about cybersecurity*. Retrieved from World Economic Forum: <https://www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges>
- Shackelford, S. J. (2009). From nuclear war to net war: Analogizing cyber attacks in international law. *Berkeley Journal of International Law*, 27, 192.
- Shafie, D. M. (2008). Participation in E-Rulemaking: Interest Groups and the Standard-Setting Process for Hazardous Air Pollutants. *Journal of Information Technology & Politics*, 5(4), 399–410. doi:10.1080/19331680802546670
- Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, 11(1), 27–49. doi:10.1007/11416-014-0231-x
- Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques* (pp. 47–53). Springer.
- Shankar, U., Chew, M., & Tygar, J. D. (2004, August). Side effects are not sufficient to authenticate software. In *USENIX Security Symposium* (Vol. 8, No. 3). USENIX.
- Shao, C., Ciampaglia, G., Flammini, A., & Menczer, F. (2016). Hoaxy: A Platform for Tracking Online Misinformation. *Proceedings of the 25th International Conference Companion on World Wide Web*, 745–750. 10.1145/2872518.2890098
- Shao, C., Hui, P., Wang, L., Jiang, X., Flammini, A., Menczer, F., & Ciampaglia, G. (2018). Anatomy of an online misinformation network. *PLoS One*, 13(4), 1–23. doi:10.1371/journal.pone.0196087 PMID:29702657
- Shapka, J. D., & Law, D. M. (2013). Does one size fit all? Ethnic differences in parenting behaviors and motivations for adolescent engagement in cyberbullying. *Journal of Youth and Adolescence*, 42(5), 723–738. doi:10.1007/10964-013-9928-2 PMID:23479327

Compilation of References

- Shariff, S., & Eltis, K. (2017). Addressing Online Sexual Violence: An Opportunity for Partnerships between Law and Education. *Education Law Journal*, 27(1).
- Shariff, S., & Hoff, D. L. (2007). Cyber bullying: Clarifying legal boundaries for school supervision in cyberspace. *International Journal of Cyber Criminology*, 1, 76–118.
- Sharma, S., Sharma, P., & Singh, G. (2018). Dark Web and Trading of Illegal Drugs. *J Forensic Science & Criminal Investigation*, 9(4), 555766. doi:0.19080/JFSCI.2018.09.555766
- Sharp, T. (2017). Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *The Journal of Strategic Studies*, 40(7), 898–926. doi:10.1080/01402390.2017.1307741
- Shea, J. (2017). How is NATO meeting the challenge of Cyberspace? *Prism*, 19–29. Retrieved from https://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/3-How_is_NATO_Meeting_Challenge_of_Cyberspace.pdf?ver=2017-12-21-110643-000
- Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, 18(1), 21–32. doi:10.1080/01972240252818207
- Sheffield, M. (2017, August 21). Big Tech, the alt-right and the unknown future of the internet. *Salon*. Retrieved from <http://www.salon.com/2017/08/21/big-tech-the-alt-right-and-the-unknown-future-of-the-internet/>
- Shen, F., & Liang, H. (2015). Cultural Difference, Social Values, or Political Systems? Predicting Willingness to Engage in Online Political Discussion in 75 Societies. *International Journal of Public Opinion Research*, 27(1), 111–124. doi:10.1093/ijpor/edu012
- Sheng, S., Wardman, B., Warner, G., Cranor, L. F., Hong, J., & Zhang, C. (2009). An empirical analysis of phishing blacklists. *Proceedings of Sixth Conference on Email and Anti-Spam (CEAS)*.
- Shenzhen Association of Online Media and China Internet Network Information Center. (2015). Retrieved June 29, 2018, from http://english.sz.gov.cn/ln/201601/t20160121_3452230.htm
- Sheridan, K. (2018, September). Cybercriminals launder up to \$200B in profit per year. *Information Week. IT Network*. Retrieved from [https://www.darkreading.com/attacks-breaches/cybercriminals-launder-up-to-\\$200b-in-profit-per-year/d/d-id/1331298](https://www.darkreading.com/attacks-breaches/cybercriminals-launder-up-to-$200b-in-profit-per-year/d/d-id/1331298)
- Sheridan, L. L. A., & Lyndon, A. E. (2010). The influence of prior relationship, gender, and fear on the consequences of stalking victimization. *Sex Roles*, 66(5-6), 340–350. doi:10.1007/11199-010-9889-9
- Shiao, V. (2017, August 1). A third of Singapore SMEs hit by ransomware last year: study. *The Business Times*. Retrieved from <https://www.businesstimes.com.sg/technology/a-third-of-singapore-smes-hit-by-ransomware-last-year-study>
- Shi, B., & Weninger, T. (2016). *Fact Checking in Heterogeneous Information Networks*. doi:10.1145/2872518.2889354
- Shin, D. H., & Kim, W. Y. (2008). Applying the technology acceptance model and flow theory to cyworld user behavior: Implication of the web2.0 user acceptance. *Cyberpsychology & Behavior*, 11(3), 378–382. doi:10.1089/cpb.2007.0117 PMID:18537514
- Shin, Y., Gupta, M., & Myers, S. A. (2011, March). The Nuts and Bolts of a Forum Spam Automator. LEET.
- Shu, K., Sliva, A., Wang, S., Tang, J. & Liu, H. (2017). Fake News Detection on Social Media: a data mining perspective. *ACM SIGKDD Explorations Newsletter*, 19(1).
- Sial, O., & Iqbal, S. (2015, November). *A Legal research guide to Pakistan*. Retrieved from <https://www.nyulawglobal.org/globalex/Pakistan.html>

- Sidbury, B. F. (2001). You've got mail...and your boss knows it: Rethinking the scope of the electronic communications privacy act. *Journal of Internet Law*, 1(5), pp16–pp22.
- Siddiqui, D. A., & Ahmed, Q. M. (2013). The effect of institutions on economic growth: A global analysis based on GMM dynamic panel estimation. *Structural Change and Economic Dynamics*, 24, 18–33. doi:10.1016/j.strueco.2012.12.001
- Siegel, L. J. (2010). *Criminology: Theories, patterns and typologies* (10th ed.). Wadsworth: Cengage Learning.
- Siegel, J., Dubrovsky, V., Kiesler, S., & McGuire, T. W. (1986). Group Processes in Computer-Mediated Communication. *Organizational Behavior and Human Decision Processes*, 37(2), 157–187. doi:10.1016/0749-5978(86)90050-6
- Siegel, L. J., & Senna, J. J. (2004). *Essentials of criminal justice* (4th ed.). Belmont: Wadsworth/Thompson learning.
- Sigler, K. (2018). Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, 12-14.
- Sijtsema, J. J., Ashwin, R. J., Simona, C. S., & Gina, G. (2014). Friendship selection and influence in bullying and defending. *Effects of moral disengagement. Developmental Psychology*, 50(8), 2093–2104. doi:10.1037/a0037145 PMID:24911569
- Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior*, 60, 35–43. doi:10.1016/j.chb.2016.02.050
- Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., . . . Hassabis, D. (2017). *Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm*. eprint arXiv:1712.01815
- Silverman, C. (2016, November 17). This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. *BuzzFeed*. Retrieved from <https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>
- Sim, R. (2018, September 20). Select Committee on fake news: 22 recommendations unveiled to combat online falsehoods. *The Straits Times*. Retrieved from <https://www.straitstimes.com/singapore/select-committee-on-fake-news-22-recommendations-unveiled-to-combat-online-falsehoods>
- Sims, J., & Xu, L. (2012). Perceived Risk of Online Shopping: Differences Between the UK and China. In *UK Academy for Information Systems Conference Proceedings* (Vol. 25). Academic Press.
- Singh, A. (2018, June 13). *CXOtoday.com*. Retrieved from CXOtoday.com: <http://www.cxotoday.com/story/ai-is-the-future-of-cybersecurity/>
- Singh, K. (2011). The 'Osama' of the internet: Anwar al-Awlaki. *Behavioural Insights*, 21.
- Singhal, A. (2012). Introducing the knowledge graph: things, not strings. *Official Google Blog*, 5.
- Singhealth, T., Attack, C., Author, C. O. I. F., Jayakumar, S., Attack, S. C., Findings, C. O. I., . . . Url, C. D. (2019). *This document is downloaded from DR-NTU, Nanyang Technological SingHealth Cyber Attack : Learning from COI Findings*. Academic Press.
- Singh, J. (2015). Violence against women in cyberworld: A special reference to India. *International Journal of Advanced Research in Management and Social Sciences*, 4(1), 60–76.
- Singh, S., Cabraal, A., & Hermansson, G. (2006). What is your husband's name?: sociological dimensions of internet banking authentication. In *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments (OZCHI '06)*. ACM. 10.1145/1228175.1228217

Compilation of References

- Singh, S., Jeong, Y.-S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, 200–222. doi:10.1016/j.jnca.2016.09.002
- Singtel. (2018, May). *Managing cyber security incidents before they become crises*. Retrieved from <https://www.singtel.com/business/singtel-global-services/content/managing-cyber-security-incidents-before-they-become-crises>
- Sinha, S. (2018). Kali Linux from the Inside Out. In *Beginning Ethical Hacking with Kali Linux* (pp. 105-135). Apress. doi:10.1007/978-1-4842-3891-2_6
- Sirianni, F. A. (1984). Was Antony's Will partially forged? *L'Antiquite Classique*, 53(1), 236–241. doi:10.3406/antiqu.1984.2126
- Sissing, S. K. (2013). *A criminological exploration of cyberstalking in South Africa (Masters thesis)*. University of South Africa. Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/13067/dissertation_sissing_sk.pdf?sequence=1
- Sjurso, I. R., Fandream, H., & Roland, E. (2016). Emotional problems in traditional and cyber victimization. *Journal of School Violence*, 15(1), 114–131. doi:10.1080/15388220.2014.996718
- Skillicorn, D. (2009). *Knowledge discovery for counterterrorism and law enforcement*. New York, NY: CRC Press.
- Skype. (2018). *Skype makes it easy to stay in touch*. Retrieved from <https://www.skype.com>
- Slaughter, R. (2018). The IT revolution reassessed part one: Literature review and key issues. *Futures*, 96, 115–123. doi:10.1016/j.futures.2017.12.006
- Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, 49(2), 147–154. doi:10.1111/j.1467-9450.2007.00611.x PMID:18352984
- Smart-contract-best-practices. (2018). Retrieved from https://consensys.github.io/smart-contract-best-practices/known_attacks/
- Smishing - Text Messaging Scams. (n.d.). Retrieved from Genisys: <https://www.genisyscu.org/files/genisys15/1/file/OnlineSecurity/SmishingTextScams.pdf>
- Smith, A., & Anderson, M. (2018, March 1). Social media use in 2018. *Pew Research Center*. Retrieved from <http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>
- Smith, C. S. (2018, May 10). Alexa and Siri Can Hear This Hidden Command. You Can't. *New York Times*. Retrieved from <https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html>
- Smith, E. J., & Kollars, N. A. (2015). QR panopticism: user behavior triangulation and barcode-scanning applications. *Information Security Journal: A Global Perspective*, 24(4-6), 157-163.
- Smith, S. (2003). From napster to kazaa: The battle over peer-to-peer filesharing goes international. *Duke law & Technology Review*, 2(1), 1–9.
- Smith. (2018). *Hacking pacemakers, insulin pumps and patients' vital signs in real time*. Retrieved September 10, 2018, from <https://www.csoononline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html>
- Smithee, M. (2009). Applying cultural concepts to academic integrity. In T. Twomey, H. White, & K. Sagendorl (Eds.), *Pedagogy, not policing: Positive approaches to academic integrity at the university* (pp. 125–134). Retrieved from http://www.academia.edu/271459/Applying_Intercultural_Concepts_to_Academic_Integrity

- Smith, H. J., Milberg, J. S., & Burke, J. S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *Management Information Systems Quarterly*, 20(2), 167–196. doi:10.2307/249477
- Smith, P. A. Jr. (1989). *On political war*. National Defense Univ.
- Smith, P. K., Del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms? In S. Bauman, D. Cross, & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, methodology* (pp. 26–40). New York, NY: Routledge.
- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, 49(4), 376–385. doi:10.1111/j.1469-7610.2007.01846.x PMID:18363945
- Smith, R. G. (2015). Trajectories of a Cybercrime. In R. Smith, R. Cheung, & L. Lau (Eds.), *Cybercrime Risk and Responses: Eastern and Western Perspectives*. London: Palgrave Macmillan. doi:10.1057/9781137474162_2
- Smith, S. G., Zhang, X., Basile, K. C., Merrick, M. T., Wang, J., Kresnow, M., & Chen, J. (2018). *The national intimate partner and sexual violence survey (NISVS): 2015 data brief*. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.
- Smooke, D. (2018). *Dealing With Reality to Get What You Want*. Retrieved from <https://hk.saowen.com/a/5fe6dc23d5b284f3604f8b7bd805473bedc84e45d02a72fd7da98b6166c986cf>
- Snapchat. (2018). *A new way to look*. Retrieved from <https://www.snapchat.com/>
- Snyder, P., Ansari, L., Taylor, C., & Kanich, C. (2016). Browser Feature Usage on the Modern Web. In *Proceedings of the 2016 Internet Measurement Conference (IMC '16)* (pp. 97-110). Santa Monica, CA: ACM. 10.1145/2987443.2987466
- Snyder, P., & Kanich, C. (2016). Characterizing fraud and its ramifications in affiliate marketing networks. *Journal of Cybersecurity*, 2(1), 71–81. doi:10.1093/cybsec/tyw006
- So, J., Kim, S., & Cohen, H. (2017). Message fatigue: Conceptual definition, operationalization, and correlates. *Communication Monographs*, 84(1), 5–29. doi:10.1080/03637751.2016.1250429
- Solairaj, A. (2016). Keyloggers software detection techniques. *Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 1–6.
- Solon, O. (2013, October). Cybercriminals launder money using in-game currencies. *Wired*. Retrieved from <http://www.wired.co.uk/article/money-laundering-online>
- Soltani, A., Cauty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. (2010). Flash Cookies and Privacy. In *AAAI Spring Symposium: Intelligent Information Privacy Management*, (pp. 158-163). AAAI.
- Song, M., Zhong, K., Zhang, J., Hu, Y., Liu, D., Zhang, W., ... Li, T. (2018). In-Situ AI: Towards Autonomous and Incremental Deep Learning for IoT Systems. *Proceedings of the IEEE International Symposium on High Performance Computer Architecture (HPCA)*, 92-103. 10.1109/HPCA.2018.00018
- Sood, A. K., & Enbody, R. J. (2013). Targeted cyber attacks: A superset of advanced persistent threats. *Security & Privacy, IEEE*, 11(1), 54–61.
- Sood, A. K., Zeadally, S., & Enbody, R. J. (2016). An Empirical Study of HTTP-based Financial Botnets. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 236–251. doi:10.1109/TDSC.2014.2382590
- Soon, C. W. T., & Goh, Z. S. S. (2017). *What Lies Beneath the Truth: A Literature Review on Fake News, False Information and More*. Institute of Policy Studies.

Compilation of References

SophosLabs 2019 Threat Report. (2018). Sophos.

Sorensen, M. S. (2018). *1,000 Danes Accused of Child Pornography for Sharing Video of Teens*. Retrieved from: <https://www.nytimes.com/2018/01/15/world/europe/denmark-child-pornography-video.html>

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In Proceedings of the 24th USENIX Security Symposium. Washington, DC: USENIX. Retrieved from <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf>

Sourander, A., Brunstein, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., ... Helenius, H. (2010). Psycho-social risk factors associated with cyberbullying among adolescents: A population-based study. *Archives of General Psychiatry*, 67(7), 720–728. doi:10.1001/archgenpsychiatry.2010.79 PMID:20603453

Southern Poverty Law Center. (2017, August 14). *Ten ways to fight hate: A community response guide*. Retrieved from <https://www.splcenter.org/20170814/ten-ways-fight-hate-community-response-guide>

Spalevic, Z., & Ilic, M. (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika (Nis)*, 63(1), 73–82. doi:10.5937/ekonomika1701073S

Special English, V. O. A. (2014, September 27). *Studying in America-31-essay mills-plagiarism* [Video file]. Retrieved from <https://www.youtube.com/watch?v=98zHYdGb-T4>

Speer, D. L. (2000). Redefining borders: The challenges to cybercrime. *Crime, Law, and Social Change*, 34(3), 259–273. doi:10.1023/A:1008332132218

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, 4(1), 71–92. doi:10.1177/1461444022226271

Spitzer, J. (2018). *Healthcare data breaches spike significantly in 7 years: 5 things to know*. Retrieved from <https://www.beckershospitalreview.com/cybersecurity/healthcare-data-breaches-spike-significantly-in-7-years-5-things-to-know.html>

Sreenivasulu, N. S. (2013). *Law Relating to Intellectual Property*. Gurugram, India: Partridge Publishing.

Srivastava, D. (2017). *What the Blue Whale Challenge's popularity tells us about vulnerable teenagers?* Retrieved October 2018, from <https://www.firstpost.com/living/what-the-blue-whale-challenges-popularity-tells-us-about-vulnerable-teenagers-3924181.html>

Srivastava, S., & Singh, A. (2011). *Facebook application development with Graph API cookbook*. Birmingham, UK: Packt Publishing.

Staab, S., Studer, R., Schnurr, H., & Sure, Y. (2001). Knowledge Processes and Ontologies. *IEEE Intelligent Systems*, 16(1), 26–34. doi:10.1109/5254.912382

Stack, B. (2018, April 9). Here's how much your personal information is selling for on the Dark Web. *Experian*. Retrieved from <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

Stake, R. (2005). Qualitative Case Studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research* (pp. 443–466). Thousand Oaks, CA: Sage Publications.

Stanton, C. (2011). Here's a project: Troll! Data! Analysis! *SuperOpinionated*. Retrieved 12th of November 2018 from <http://superopinionated.dreamhosters.com/2011/02/08/here-is-a-project-troll-data-analysis>

Stanton, L. (2014, August 18). Effect of “right to be forgotten” on free expression sparks debate. Cybersecurity Policy Report.

- Starks, T. (2018). Sizing up Chinese, North Korean cyberattacks. *Politico*. Retrieved from <https://www.politico.com/newsletters/morning-cybersecurity/2018/06/15/sizing-up-chinese-north-korean-cyberattacks-252481>
- Statement of Principles on Access to Evidence and Encryption. (2018, August 29). Retrieved from <https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption>
- Statista. (2017). *Share of women worldwide who have ever experienced abuse or harassment on selected websites and social media platforms as of July 2017*. Retrieved from <https://www.statista.com/statistics/784821/harassment-women-websites-social-media-platforms/>
- Statista. (2018). Global digital population as of October 2018 (in millions). *Demographics & Use*. Available at: <https://www.statista.com/statistics/617136/digital-population-worldwide/>
- Statista. (2018). *Number of social network users worldwide from 2010 to 2021 (in billions)*. Retrieved from <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>
- Stavroulia, K. E., Harisiou, A. R., Manouchou, E., Georgiou, K., Sella, F., & Lanitis, A. (2016). A 3D Virtual Environment for Training Teachers to Identify Bullying. *Proceedings of the 18th Mediterranean Electrotechnical Conference MELECON 2016*. 10.1109/MELCON.2016.7495417
- Stefanie, O. (2001). Reversal of fortune – tracking web trackers. *ZD Net News*. Retrieved October 6 2018, from <http://www.zdnet.com/zdnn/stories/news/0,4586,2692472,00.html>
- Steil, M. (2005). 17 mistakes Microsoft made in the Xbox security system. *22nd Chaos Communication Congr.*
- Stephenson, P., & Smith, D. (1989). Bullying in the junior school. In D. P. Tattum & D. A. Lane (Eds.), *Bullying in schools* (pp. 45–48). Stoke-on-Trent, UK: Trentham Books.
- Stericycle Expert Solutions. (2019). *Recall index, Q4, 2018*. Retrieved from <https://www.stericycleexpertsolutions.com/wp-content/uploads/2019/02/ExpertSolutions-RecallIndex-Q42018-web.pdf>
- Steve. (2018, March 21). Canada allocates \$1 Billion to Safeguard against cybercrime. *DarkWebNews*. Retrieved from <https://darkwebnews.com/cyber-security/1-billion-against-cybercrime-canada/>
- Stevens, M., & Dujanovic, D. (2018, October 26). Homebuyers targeted by sophisticated, billion dollar hacking scheme. *KSL*. Retrieved from <https://www.ksl.com/article/46414717/homebuyers-targeted-by-sophisticated-billion-dollar-hacking-scheme>
- Stiegler, B. (2018). *The Neganthropocene*. Open Humanities Press.
- Stiglitz, G. (1990). *Protección Jurídica del Consumidor*. Buenos Aires: Depalma.
- Stoecklin, M. P. (2018, August 8). *DeepLocker: How AI Can Power a Stealthy New Breed of Malware*. Retrieved from <https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/>
- Stokes, M., & Hsiao, R. (2013). *The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics*. Project 2049 Institute.
- Stoll, L. C., & Block, R. Jr. (2015). Intersectionality and cyberbullying: A study of cybervictimization in a Midwestern high school. *Computers in Human Behavior*, 52, 387–391. doi:10.1016/j.chb.2015.06.010
- Stop Violence Against Women. (2018). *Trafficking in Women. Stop Violence Against Women: A Project of the Advocates for Human Rights*. Retrieved December 1, 2018 from http://www.stopvaw.org/trafficking_in_women

Compilation of References

- Storey, J. E., & Hart, S. D. (2011). How Do Police Respond to Stalking? An Examination of the Risk Management Strategies and Tactics Used in a Specialized Anti-Stalking Law Enforcement Unit. *Journal of Police and Criminal Psychology*, 26(2), 128–142. doi:10.1007/11896-010-9081-8
- Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly*, 93(2), 296–311. doi:10.1177/1077699016630255
- Strandh, M. (2000). *Varying unemployment experiences? The economy and mental well-being*. Umeå University Department of Sociology.
- Strategy for a Technology-driven Future. (2017, November 3). *Infocomm Media Development Authority*. Retrieved from <https://www.imda.gov.sg/infocomm-and-media-news/buzz-central/2016/6/strategy-for-a-technology-driven-future>
- Straub, D. W., & Collins, R. W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *Management Information Systems Quarterly*, 14(2), 143–156. doi:10.2307/248772
- Strauss, A. L. (1987). Codes and Coding. In *Qualitative analysis for social scientists* (pp. 55–81). Cambridge University Press. doi:10.1017/CBO9780511557842.004
- Strayer, W. T., Lapsley, D. E., Walsh, R., & Livadas, C. (2008). Botnet detection based on network behavior. *Springer Advances in Information Security*, 36, 1–24.
- Stroebe, W., Postmes, T., & Spears, R. (2012). Perspectives on Psychological Science. *Scientific Misconduct and the Myth of Self-Correction in Science*, 7, 670–688. doi:10.1177/1745691612460687
- Strohmeier, D., Aoyama, I., Gradinger, P., & Toda, Y. (2013). Cybervictimization and cyberaggression in Eastern and Western countries: Challenges of constructing a cross-cultural appropriate scale. In S. Bauman, D. Cross, & J. L. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, and methodology* (pp. 202–221). New York: Routledge.
- Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., . . . Wolf, R. D. (2017). *Finding Cyber Threats with ATT&CK-Based Analytics*. MTR170202 MITRE Technical Report. Retrieved May 16, 2019, from <https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf>
- Strong, D. M., & Volkoff, O. (2010). Understanding Organization—Enterprise system fit: A path to theorizing the information technology artifact. *Management Information Systems Quarterly*, 34(4), 731–756. doi:10.2307/25750703
- Stuart, K. (2013). Xbox One DRM restrictions dropped after gamer outcry. *The Guardian*.
- Stutzman, F. (2006). An evaluation of identity-sharing behaviour in social network communities. *Journal of the International Digital Media and Arts Association*, 3(1), 10–18.
- Subrahmanian, V. S., Ovelgonne, M., Dumitras, T., & Prakash, B. A. (2013). *The Global Cyber-Vulnerability Report, no. November 2013*. Cham: Springer International Publishing.
- Sui, D., Caverlee, J., & Rudesill, D. (2015). *The Deep Web and Darknet: A look inside the internet's massive black box*. Academic Press.
- Suleimanov, A., Abramov, M., & Tulupyeu, A. (2018). *Modelling of the social engineering attacks based on social graph of employees communications analysis*. In *IEEE Industrial Cyber-Physical Systems*. St. Petersburg, Russia: ICPS.
- Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, 7(3).

Summary of the HIPAA Security Rule | HHS.gov. (2013). Retrieved from <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

Summo3000. (2018). *Top 20 Countries Found to Have the Most Cybercrime*. Retrieved May 12, 2019, from <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>

Sumner, C., Byers, A., Boochever, R., & Park, G. J. (2012). Predicting dark triad personality traits from Twitter usage and a linguistic analysis of Tweets. *Proceedings at the IEEE 11th International Conference on Machine Learning and Applications (ICMLA)*, 386-393. 10.1109/ICMLA.2012.218

Sun, W., Nasraoui, O., & Shafto, P. (2018). Iterated Algorithmic Bias in the Interactive Machine Learning Process of Information Filtering. In *Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. Seville, Spain: SCITEPRESS - Science and Technology Publications. 10.5220/0006938301100118

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013, April). Unlocking the privacy paradox: do cognitive heuristics hold the key? In CHI '13 extended abstracts on human factors in computing systems (pp. 811-816). doi:10.1145/2468356.2468501

Suneja, K. (n.d.). *Left wing extremism, border tensions challenging for India: Arun Jaitley*. Retrieved from economictimes.indiatimes.com/articleshow/5857661.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Supan, Q. M. H. (2015, March 10). Cyber crimes. *The Daily Star*. Retrieved from <https://www.thedailystar.net/law-our-rights/cyber-crimes-70592>

Sutcliffe, A., Binder, J., & Dunbar, R. (2018). Activity in social media and intimacy in social relationships. *Computers in Human Behavior*, 85, 227–235. doi:10.1016/j.chb.2018.03.050

Sutherland, E., & Cressey, D. (1960). *Principles of criminology* (6th ed.). Philadelphia: J.B. Lippincott.

Sven, Marcan, & Comex. (2013). Console hacking 2013: WiiU. *30th Chaos Communication Congr*. Retrieved from http://media.ccc.de/browse/congress/2013/30C3_-_5290_-_en_-_saal_2_-_201312272030_-_console_hacking_2013_-_sven_-_marcan_-_nicholas_allegria_comex.html

Swaminathan, R. (2014). Politics of Technoscapes: Algorithms of Social Inclusion & Exclusion in a Global City. *Journal of International & Global Studies*, 6(1), 90-105. Retrieved 12th of November 2018 from <http://www.lindenwood.edu/files/resources/90-105.pdf>

Swan, M. (2018). Blockchain Economic Networks: Economic Network Theory—Systemic Risk and Blockchain Technology. *Business Transformation through Blockchain*, 3–45. doi:10.1007/978-3-319-98911-2_1

Sweeney, L. (2000). *Uniqueness of simple demographics in the U.S. Population*. Carnegie Mellon University, Laboratory for Internal Data Privacy. Retrieved October 13, 2018, from <https://dataprivacylab.org/projects/identifiability/paper1.pdf>

Sweeney, M. (2014). *What the Law Can (and Can't) Do About Online Harassment*. Retrieved 12th of November 2018 from <https://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/>

Sweeten, G., Bushway, S. D., & Paternoster, R. (2009). Does dropping out of school mean dropping into delinquency? *Criminology*, 47(1), 47–91. doi:10.1111/j.1745-9125.2009.00139.x

Symantec Corporation. (2017). Good cyber hygiene. *Norton by Symantec*. Retrieved from <https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html>

Compilation of References

Symantec White Paper - Turning the Tables on Malware. (2012). Retrieved June 22, 2018, from https://www.symantec.com/content/en/us/enterprise/white_papers/b-turning_the_tables_on_malware_WP_21155056.en-us.pdf

Symantec. (2016). *Cyber Crime and Cyber Security Trends in Africa*. Retrieved from www.symantec.co/theme/cyber-security-trends-africa

Syverson, P., Dingledine, R., & Mathewson, N. (2004). Tor: The second generation onion router. Usenix Security.

Szabo, N. (1997). *The Idea of Smart Contracts*. Retrieved from <http://www.fon.hum.uva.nl/rob/Courses/InformationIn-Speech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>

Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014). Intriguing properties of neural networks. *International Conference on Learning Representations*.

Szekely, P., Knoblock, C. A., Slepicka, J., Philpot, A., Singh, A., Yin, C., ... Stallard, D. (2015, October). Building and using a knowledge graph to combat human trafficking. In *International Semantic Web Conference* (pp. 205-221). Springer. 10.1007/978-3-319-25010-6_12

Tachini, E., Ballarin, G., Vedova, M., Moret, S., & de Alfaro, L. (2017). *Some Like it Hoax: automated fake news detection in social networks*. arXiv preprint: 1704.07506

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, 23(4), 689–705. doi:10.2478/13374-013-0158-9

Takahashi, D. (2013). *Nintendo sold 2.4M wii-U consoles in 9 months. Less than Sony and Microsoft sold in 6 weeks*. Retrieved from <http://venturebeat.com/2014/01/29/nintendo-sold-2-4m-wii-u-consoles-in-9-months-less-than-sony-and-microsoft-sold-in-six-weeks/>

Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. (2017). A Review of Smart Cities Based on the Internet of Things Concept. *Energies*, 10(4), 1–23. doi:10.3390/en10040421

Taleb, N. (2017). Election predictions as martingales: An arbitrage approach. *Quantitative Finance*, 18(1), 1–5. doi:10.1080/14697688.2017.1395230

Tamkin, E. (2017). 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? *Foreign Policy*. Retrieved from <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>

Tan, G., Wan, W. P., & Teo, J. (2014). *SURE Campaign: Promoting Information Literacy Awareness to Singaporeans*. Presented at the IFLA WLIC 2014 - Lyon - Libraries, Citizens, Societies: Confluence for Knowledge.

Tan, C. W. T., & Wang, P. (2017). *The psychology of ransomware: Manipulation of human emotion for criminal activity (HTBSC Research Report 02/2017)*. Singapore: Home Team Behavioural Sciences Centre.

Tandoc, E., Lim, Z., & Ling, R. (2017). Defining “fake news” a typology of scholarly definitions. *Digital Journal*, 6, 1–17.

Tan, E. E. G., & Ang, B. (2017). *Clickbait: Fake News and Role of the State*. RSIS.

Tangen, D., & Campbell, M. (2010). Cyberbullying prevention: One primary school's approach. *Australian Journal of Guidance & Counselling*, 20(2), 225–234. doi:10.1375/ajgc.20.2.225

Tannery, A. (2016). *Your Money: Cyber bullying delivers a punch to consumer wallets*. Reuters.

Tan, O. S. L., Khan, S., & Abdul Rahim, R. (2014). Internet: The double-edged sword of trafficking of women in Malaysia. *Pertanika Journal of Social Science & Humanities*, 22, 149–160.

- Tapanainen, T. (2017). *Sense-making in Cyber Security—Examining Responder Behaviors in Cyber-Attacks*. Academic Press.
- Tarnovsky, C. (2010). Semiconductor security awareness today and yesterday. *Blackhat 2010*.
- Tarnovsky, C. (2012). Attacking tpm part two. *Defcon 2012*.
- Taşkın, Ş. C. (2008). *Bilişim Suçları*. İstanbul: Beta Yayınevi.
- Tasman-Jones, J. (2016, March 31). Human behaviour still biggest cause of cybercrime. *Fund Strategy*. Retrieved from <https://www.fundstrategy.co.uk/human-behaviour-still-biggest-cause-of-cybercrime/>
- Taub, A., & Fisher, M. (2018, April 21). Where Countries Are Tinderboxes and Facebook Is a Match - The New York Times. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/04/21/world/asia/facebook-sri-lanka-riots.html>
- Taylor, M., & Quayle, E. (2003). *Child Pornography. An Internet Crime*. Brunner-Routledge.
- Taylor. (2004). Hacktivism – Resistance is Fertile? In *The Blackwell Companion to Criminology*. Malden, MA: Blackwell Pub.
- Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2010). *Digital crime and digital terrorism* (2nd ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Tee, Z. (2018, September 19). Bitcoin scam online using fake comments attributed to Tharman: MAS. *The Straits Times*. Retrieved from <https://www.straitstimes.com/business/bitcoin-scam-online-using-fake-comments-by-tharman-mas>
- Tee, S. H., Neo, L. S., Chin, J., & Khader, M. (2018). *Defeated but alive: The latent threat of ISIS (HTBSC research report 16/2018)*. Singapore: Home Team Behavioural Sciences Centre.
- Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. K. (2016). A survey on touch dynamics authentication in mobile devices. *Computers & Security*, 59, 210–235.
- Tellenbach, B., Paganoni, S., & Rennhard, M. (2016). Detecting obfuscated JavaScripts from known and unknown obfuscators using machine learning. *International Journal on Advances in Security*, 9(3/4), 196–206.
- Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, 23(4), 1836–1846. doi:10.1109/TPWRS.2008.2002298
- Tennakoon, H., Saridakis, G., & Mohammed, A.-M. (2018). Child Online Safety and Parental Intervention: A Study of Sri Lankan Internet Users. *Information Technology & People*, 31(3), 770–790. doi:10.1108/ITP-09-2016-0213
- Tepper, B. J. (2000). Consequences of Abusive Supervision. *Academy of Management Journal*, 43(2), 178–190.
- Terre Blanche, M., & Durrheim, K. (1999). Social constructionist methods. *Research in practice: Applied methods for the social sciences*, 147–172.
- Terre des hommes. (2018). *Sweetie: how to stop Webcam Child Sex Tourism*. Retrieved from <https://www.tdh.ch/en/projects/sweetie-how-stop-webcam-child-sex-tourism>
- Terrovitis, M., Mamoulis, N., & Kalnis, P. (2008). Privacy-preserving anonymization of set-valued data. *Proceedings of the VLDB Endowment International Conference on Very Large Data Bases*, 1(1), 115–125. doi:10.14778/1453856.1453874
- Thales eSecurity. (2018). *2018 Thales Data Threat Report*. 451 Research. Retrieved from <http://go.thalesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf>

Compilation of References

- Thales. (2018). 2018 Thales data threat report global edition. *Thales*. Retrieved from https://dtr.thalessecurity.com/?utm_source=google&utm_medium=cpc&utm_campaign=DTR&utm_term=%7BKeyword%7D&gclid=EAIaIQobChMImZPBncjH3QIVEInICh1hCAMEEAMYASAAEgKN8_D_BwE
- Tham, I. (2018). Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack. *The Straits Times*. Retrieved from <https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most>
- Theoharis, M. (2015). *Laws on federal fraud*. Retrieved from <http://www.criminaldefenselawyer.com/crime-penalties/federal/federal-fraud.htm>
- Thomas, S. B. (2000). *The Legacy of Tuskegee. The Body: The Complete HIV/AIDS Resource*. Retrieved from <http://www.thebody.com/content/art30946.html>
- Thomas, L. D., Vernet, A., & Gann, D. M. (2016). Adoption readiness in service innovation: The case of digital money. *Industry and Innovation*, 23(4), 353–381. doi:10.1080/13662716.2016.1156519
- Thornberg, R., & Jungert, T. (2013). Bystander behavior in bullying situations: Basic moral sensitivity, moral disengagement and defender self-efficacy. *Journal of Adolescence*, 36(3), 475–483. doi:10.1016/j.adolescence.2013.02.003 PMID:23522703
- Thrive Analytics. (2018). Retrieved from <http://www.thriveanalytics.com/Press%20Releases-%202014%20Digital%20Wallet%20Usage%20Study.html>
- Thukral, S. (2017). Unfolding Bitcoin. *International Journal Of Research In Commerce & Management*, 8(2), 32–33.
- Tiku, N. (2017, August 26). Alt-Right Chat Logs Are Key to Charlottesville Lawsuits. *Wired*. Retrieved from <https://www.wired.com/story/leaked-alt-right-chat-logs-are-key-to-charlottesville-lawsuits/>
- Tilley, A. (2017, February 16). Amazon Alexa Can Now Unlock Your Doors. *Forbes*. Retrieved from <https://www.forbes.com/sites/aarontilley/2017/02/16/amazon-alexa-can-now-unlock-your-front-door/#6c75556875f1>
- Tillyer, M. S., & Eck, J. E. (2009). Routine activities. *21st Century Criminology: A Reference Handbook*, 1, 279–287.
- Timberg, C., Romm, T., & Dwoskin, E. (2018, April 4). Facebook: 'Malicious actors' used its tools to discover identities and collect data on a massive global scale. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.0cf79dfa7abf
- Tinder. (2018). *Match. Chat. Date*. Retrieved from <https://tinder.com>
- Toben, Gerald Frederick v State of Victoria & Allen, Graham, No. CCA 10 of 1989 (Supreme Court of Victoria, Appeal Division 1990).
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277–287. doi:10.1016/j.chb.2009.11.014
- Tokunaga, R. S., & Aune, K. S. (2017). Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking. *Journal of Interpersonal Violence*, 32(10), 1451–1475. doi:10.1177/0886260515589564 PMID:26082443
- Toledano, S., Werch, B. L., & Wiens, B. A. (2015). Domain-specific self-concept in relation to traditional and cyber peer aggression. *Journal of School Violence*, 14(4), 405–423. doi:10.1080/15388220.2014.935386
- Tomar, D. (2012). *The shadow scholar: How I made a living helping college kids cheat*. New York, NY: Bloomsbury.

- Tomeo, F. (2014). *Redes Sociales y Tecnologías 2.0*. Buenos Aires: Astrea.
- Tomeo, F. (2010). *Las redes sociales y su régimen de responsabilidad civil*. Buenos Aires: La Ley.
- Tompkins, T. (2017, September). Fraudsters target video games for credit card fraud. *CreditCards.com*. Retrieved from <https://www.creditcards.com/credit-card-news/how-to-prevent-video-game-credit-card-fraud.php>
- Toney-Butler, T. J., & Mittel, O. (2018). *Human Trafficking*. Treasure Island, FL: StatPearls Publishing. Retrieved April 1, 2019 from <https://www.ncbi.nlm.nih.gov/books/NBK430910/>
- Tonon, A., Demartini, G., & Cudré-Mauroux, P. (2012, August). Combining inverted indices and structured search for ad-hoc object retrieval. In *Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval* (pp. 125-134). ACM. 10.1145/2348283.2348304
- Top 10-2017 Details About Risk Factors - OWASP. (2017). Retrieved December 6, 2018, from https://www.owasp.org/index.php/Top_10-2017_Details_About_Risk_Factors
- TOR (anonymity network) Wiki. (2018). Retrieved 2nd December, 2018, from [https://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](https://en.wikipedia.org/wiki/Tor_(anonymity_network))
- Totura, C. M. W., MacKinnon-Lewis, C., Gesten, E. L., Gadd, R., Divine, K. P., Dunham, S., & Kamboukos, D. (2009). Bullying and victimization among boys and girls in middle school: The influence of perceived family and school contexts. *The Journal of Early Adolescence*, 29(4), 571–609. doi:10.1177/0272431608324190
- Toyo, D. O. (2017). ICT Use and Its Impact in Combating Cybercrimes in Abraka, Delta State. *Nigeria Research Journal of Mass Communication and Information Technology*, 3(1), 10–23.
- Tran, T. P., Tsai, P., Jan, T., & He, X. (2012). Machine Learning Techniques for Network Intrusion Detection. In I. Management Association (Ed.), *Machine Learning: Concepts, Methodologies, Tools and Applications* (pp. 498-521). Hershey, PA: IGI Global. doi:10.4018/978-1-60960-818-7.ch310
- Trend Micro. (2015, January). *Data privacy and online gaming: Why gamers make for ideal targets*. Retrieved from <http://www.trendmicro.com/vinfo/us/security/news/online-privacy/data-privacy-and-online-gaming-why-gamers-make-for-ideal-targets>
- Trend Micro. (2016, October). *The cybercriminal roots of selling online gaming currency*. Retrieved from <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-roots-selling-online-gaming-currency>
- Trend Micro. (2017). *Cybercrime and Other Threats Faced by the Healthcare Industry – a TrendLabs Research Paper*. Retrieved from <https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf> Accessed 25 March 2019.
- Trenholm, S. (2007). A review of cheating in fully asynchronous online courses: A math or fact-based course perspective. *Journal of Educational Technology Systems*, 35(3), 281–300. doi:10.2190/Y78L-H21X-241N-7Q02
- Truta, T. M., & Vinay, B. (2006). Privacy protection: p-sensitive k-anonymity property. In Null (p. 94). IEEE.
- Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology*, 44(1), 66–91. doi:10.1093/bjc/44.1.66
- Tseng, Y. M. (2007). An efficient two-party identity-based key exchange protocol. *Informatica*, 18(1), 125–136.
- Tumblr. (2018). Come for what you love. Stay for what you discover. Retrieved from <https://www.tumblr.com/>

Compilation of References

- Turner, A., & Irwin, A. S. (2018). Bitcoin transactions: A digital discovery of illicit activity on the blockchain. *Journal of Financial Crime*, 25(1), 109–130. doi:10.1108/JFC-12-2016-0078
- Turner, R., & Eden, A. H. (2008). The Philosophy of Computer Science. *Journal of Applied Logic*, 6(4), 459–626. doi:10.1016/j.jal.2008.09.006
- Turvey, B. E. (2011). Modus Operandi, Motive, and Technology. In *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Amsterdam: Elsevier.
- Twitter. (2018). *See what's happening in the world right now*. Retrieved from <https://twitter.com>
- U.S. Department of Justice. (2017). Victims of Identity Theft. Retrieved from <https://www.bjs.gov/content/pub/pdf/vit14.pdf>
- U.S. Department of State. (2018). *Trafficking in Persons Report June 2018*. Retrieved from <https://www.state.gov/documents/organization/282802.pdf>
- U.S. Government Accountability Office. (2018). *Human Trafficking: State and USAID Should Improve Their Monitoring of International Counter-Trafficking Projects*. GAO-19-77. Retrieved from <https://www.gao.gov/products/GAO-19-77>
- U.S. Government. (1988). *Selling or buying of children*, 18 U.S. Code § 2251A § (1988). Retrieved from <https://www.law.cornell.edu/uscode/text/18/2251A>
- U.S. Government. (2000). *Sex trafficking of children or by force, fraud, or coercion*, 18 U.S. Code § 1591 § (2000). Retrieved from <https://www.law.cornell.edu/uscode/text/18/1591>
- Udoka, C. O., & Ogege, S. (2012). Public debt and the crisis of development in Nigeria econometric Investigation. *Asian Journal of Finance and Accounting*, 4(2), 231–243. doi:10.5296/ajfa.v4i2.2028
- UK House of Commons Library. (2018). *Misogyny as a hate crime, A Westminster Hall debate on Misogyny as a hate crime is scheduled for Wednesday 7 March 2018 at 9.30am. The Member leading the debate is Melanie Onn MP*. Available at <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CDP-2018-0057>
- UK House of Commons. (2017). *Online harassment and cyberbullying by Pat Strickland and Jack Dent, Number 07967*. Author.
- UK House of Commons. (2018). *Misogyny as a Hate Crime, Number CDP-2018-0057*. Author.
- Ullmann, M. (1994). *L'État, c'est nous*. Paris: Calmann-Lévy.
- Uma, M. S. (2017, April). Outlawing cybercrimes against women in India. *Bharati Law Review*, 103-116.
- UN Broadband Commission for Digital Development Working Group on Broadband and Gender. (2015). *Cyber Violence Against Women and Girls A World-Wide Wake-Up Call*. Retrieved 12th of November 2018 from <https://en.unesco.org/sites/default/files/genderreport2015final.pdf>
- UN Broadband Commission. (2015). *Cyber violence against women and girls: A worldwide wake-up call*. Geneva: ITU & UNESCO. Retrieved from <https://en.unesco.org/sites/default/files/genderreport2015final.pdf>
- UN Department of Peacekeeping Operations. (2015). *The Protection of Civilians in United Nations Peacekeeping*. United Nations.
- UN General Assembly. (1948). Universal Declaration of Human Rights. Retrieved from <https://www.un.org/en/universal-declaration-human-rights/index.html>
- UN GGE. (2013, June 24). *Development in the Field of Information and Telecommunications in the context of international Security*. New York: United Nations Publications.

UN Human Rights Council. (2016). Resolution on the promotion, protection and enjoyment of human rights on the Internet. Retrieved from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

UN Women. (2016). *Indecent representation of women (Prohibition) Act*. Retrieved 12th of November 2018 <http://evaw-global-database.unwomen.org/en/countries/asia/india/1986/indecent-representation-of-women--prohibition--act-1986>

UN. (2001, January 22). *UN General Assembly*. Retrieved from A/Res/55/63: Http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

UN. (2003, December 18). *UN General Assembly Resolution*. Retrieved from A/Res/ 58/32.

UNESCO. (2015). *Combating Online Violence Against Women & Girls: A Worldwide Wake-up Call Highlights*. Retrieved 12th of November 2018 from <https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf>

United Nations Conference on Trade and Development. (n.d.). *Cybercrime Legislation Worldwide*. Retrieved December 6, 2018, from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

United Nations Department of Peacekeeping Operations. (2014). *Planning Toolkit*. United Nations.

United Nations Office on Drugs and Crime. (2010). *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. Vienna: Studies and Threat Analysis Section, Policy Analysis and Research Branch, Division for Policy Analysis and Public Affairs, UNODC. Retrieved from https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

United Nations Office on Drugs and Crime. (2012, July 19). *Human trafficking: organized crime and the multibillion dollar sale of people*. Retrieved December 4, 2018 from http://www.unodc.org/unodc/en/frontpage/2012/July/human-trafficking_organized-crime-and-the-multibillion-dollar-sale-of-people.html

United Nations Office on Drugs and Crime. (2018). *Introduction*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_2_GLOBAL.pdf

United Nations Office on Drugs and Crime. (n.d.). *Global Overview Of Drug Demand And Supply, Latest trends, cross-cutting issues*. Retrieved from https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_2_GLOBAL.pdf

United Nations. (1989). *Convention on the Rights of the Child*. Retrieved from <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>

United Nations. (1990). *Special Rapporteur on the sale of children*. Retrieved from <https://www.ohchr.org/en/issues/children/pages/childrenindex.aspx>

United Nations. (1992). *An Agenda for Peace A/47/277*. Author.

United Nations. (2000). *Crimes related to computer networks*. Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Retrieved December 6, 2018, from https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf

United Nations. (2000). *Optional Protocol to the Convention on the Rights of the Child*. Retrieved from <https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx>

United Nations. (2000). *United Nations Convention Against Transnational Organized Crime*. Retrieved December 1, 2018 from https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

United Nations. (2005). *The Millennium Development Goals Report*. New York: United Nations Publications.

Compilation of References

United Nations. (2008). *United Nations Peacekeeping Operations: Capstone Doctrine*. Author.

United Nations. (2016). *Global Report on Trafficking in Persons*. Retrieved from https://www.unodc.org/documents/data-and-analysis/glotip/2016_Global_Report_on_Trafficking_in_Persons.pdf

United States Bureau of Labor Statistics. (2018). Information security analysts job outlook. *Occupational Outlook Handbook*. Retrieved from <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>

United States Department of State. (1987). Soviet influence activities: a report on active measures and propaganda, 1986-87 (Vol. 9627). US Department of State.

United States Homeland Security. (2009). *Developing an Industrial Control Systems Cybersecurity Incident Response Capability*. Author.

United States Information Agency. (1988). *Soviet Active Measures in the Era of Glasnost*. Retrieved from <http://inside-thecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20in%20the%20Era%20of%20Glasnost%20March%201988.pdf>

United States of America v. Bilal Abood. (2015). *Indictment No. 3-15CR-0256K: In the United States District Court for the Northern Division of Texas Dallas Division-Filed June 10, 2015*. Retrieved from http://www.investigativeproject.org/documents/case_docs/2747.pdf

United States v. O'Brien, 391 U.S. 367 (1968). *Yahoo! Inc. v. La Ligue Contre Le Racisme*, 169 F. Supp. 2d 1181 - Dist. Court, (ND Cal., 2001).

United v. Microsoft Corps., 584, U.S. (2018). Retrieved October 28, 2018, from <https://supreme.justia.com/cases/federal/us/584/17-2/case.pdf>

University of Warwick & TNO. (2017). Policing the Dark Web: Ethical and legal issues. *Medi@4SEC*. Retrieved from <http://media4sec.eu/downloads/d4-3.pdf>

UNODC. (2013). *Comprehensive Study on Cybercrime*. Vienna: United Nations.

Unsgaard, E., & Meloy, J. R. (2011). The Assassination of the Swedish Minister for Foreign Affairs. *Journal of Forensic Sciences*, 56(2), 555–559. doi:10.1111/j.1556-4029.2010.01653.x PMID:21210810

Updated: List of Dark Net Markets (Tor & I2P). (2018, October 15). Retrieved November 3, 2013, from <https://www.deepdotweb.com/2013/10/28/updated-list-of-hidden-marketplaces-tor-i2p/>

Urbas, G. (2010). Protecting Children From Online Predators: The Use of Covert Investigation Techniques by Law Enforcement. *Journal of Contemporary Criminal Justice*, 26(4), 410–425. doi:10.1177/1043986210377103

US Attorney General. (1999). *Cyberstalking: A new challenge for law enforcement and industry*. Author.

US GAO. (2010). *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*. United States Government Accountability Office. Retrieved November 2, 2018, from <https://www.gao.gov/new.items/d10606.pdf>

US Sixth Circuit. (2016). *USA Vs Farid Fata. File Name: 16a0283n.06*. Retrieved from <https://www.gpo.gov/fdsys/pkg/USCOURTS-ca6-15-01935/pdf/USCOURTS-ca6-15-01935-0.pdf>

USA Office of the Director of National Intelligence. (2017). *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

- US-CERT. (2018). Avoiding Social Engineering and Phishing Attacks. Retrieved from <https://www.us-cert.gov/ncas/tips/ST04-014>
- Usmanov, R. (2017). *Sběr, transformace a integrace dat z domény*. Academic Press.
- Ustbmde. (2018). *Smart Contract*. Retrieved from <https://bitbucket.org/ustbmde/smartcontract/wiki/Home>
- Vacha, D., Saikat, G., & Yin, Z. (2013). ViceROI: Catching Click-Spam in Search Ad Networks. In *ACM Conference on Computer and Communications Security* (pp. 765-776). New York, NY: ACM. doi:10.1145/2508859.2516688
- Vaishnavi, V., & Kuechler, B. (2015). *Design Science Research in Information Systems*. Academic Press.
- Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your apps know where you were last night, and they're not keeping it secret. *The New York Times*, Retrieved from <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?mtrref=www.google.com&linked=google>
- Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press. doi:10.1093/acprof:oso/9780190204792.001.0001
- Van Blarcum, C. D. (2005). Internet Hate Speech: The European Framework and the Merging American Haven. *Washington and Lee Law Review*, 2, 804.
- Van Buskirk, J., Naicker, S., Bruno, R., Burns, L., Breen, C. & Roxburgh, A. (2016). Drugs and the Internet. *Citation*, 2016(7).
- Van de Verden, P. G., Pecoraro, M., Houwerzijl, M. S., & van der Meulen, E. (2018). (in press). Mental health problems among whistleblowers: A comparative study. *Psychological Reports*. doi:10.1177/0033294118757681 PMID:29451073
- van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407–412. doi:10.1089/cyber.2017.0028 PMID:28657783
- Van der Aalst, W. M. P. (2016). *Process Mining: Data Science in Action*. Springer. doi:10.1007/978-3-662-49851-4
- Van der Zwaan, J., Jonker, C.M., & Dignum, V. (2010). Simulating Peer Support for Victims of Cyberbullying. *New Phythologist*.
- Van Dongen, S. (1998). *A new cluster algorithm for graphs*. Centrum voor Wiskunde en Informatica.
- Van Hee, C., Jacobs, G., Emmery, C., Desmet, B., & Lefever, E., Verhoeven, B., ... & Hoste, V. (2018). Automatic detection of cyberbullying in social media text. *PLoS One*, 1–22. doi:10.1371/journal.pone.0203794 PMID:30296299
- Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *The International Journal on Drug Policy*, 24(5), 385–391. doi:10.1016/j.drugpo.2013.01.005 PMID:23465646
- Váradi-Csema, E. (2013). Gyermek- és fiatalkori bűnözés alapkérdései, különös tekintettel a serdülőkor pszichés sajátosságaira. In Á. Farkas (Ed.), *Tanulmányok a bűnügyi tudományok köréből* (pp. 5–42). Miskolc, Hungary: Gazdász Elasztik.
- Váradi-Csema, E. (2016). A gyermek- és fiatalkori kriminalitás. In A. Borbíró, K. Gönczöl, K. Kerecsi, & M. Lévy (Eds.), *Kriminológia* (pp. 616–651). Budapest, Hungary: Wolters Kluwer.
- Varghese, G. (2016). A sociological study of different types of cyber crime. *International Journal of Social Science and Humanities Research*, 4(4), 599–607.
- Vargiu, E., & Urru, M. (2012). Exploiting web scraping in a collaborative filtering-based approach to web advertising. *Artificial Intelligence Review*, 2(1), 44.

Compilation of References

- Varma, V. (2007). Use of ontologies for organizational knowledge management and knowledge management systems. In R. Sharman, R. Kishore, & R. Ramesh (Eds.), *Ontologies* (vol. 14, pp. 21-27). Berlin: Springer. doi:10.1007/978-0-387-37022-4_2
- Varshney, G., Misra, M., & Atrey, P. K. (2016). A survey and classification of web phishing detection schemes. *Security and Communication Networks*, 9(18), 6266–6284. doi:10.1002/ec.1674
- Vartabedian, M., Wells, G., & O'Reilly, L. (2018, July 1). Businesses Blast California's New Data-Privacy Law. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/businesses-blast-californias-new-data-privacy-law-1530442800>
- Vasconcelos, L. E. G., Franco Rosa, F., Kusumoto, A. Y., Duarte, L. O., & Silva, P. A. L. (2013). Social network analysis for social engineering footprinting. In *Proceedings of the 8^a Conferência Ibérica de Sistemas e Tecnologias de Informação*, (vol. 2, pp. 185-190). Lisboa: Academic Press.
- Vasquez, I., & Porcnik, T. (2017). *The Human Freedom Index 2017: A Global Measurement of Personal, Civil, and Economic Freedom*. Washington, DC: Cato Institute, Fraser Institute, and the Friedrich Naumann Foundation for Freedom.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly*, 27(3), 425–478. doi:10.2307/30036540
- Venkatesh, V., Thong, J. Y., Chan, F. K., Hu, P. J., & Brown, S. A. (2011). Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context. *Information Systems Journal*, 21(6), 527–555. doi:10.1111/j.1365-2575.2011.00373.x
- Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *Management Information Systems Quarterly*, 36(1), 157–178. doi:10.2307/41410412
- Venkiteswaran, G. (2018, September 23). Fake news still a crime in Malaysia. *The Star Online*. Retrieved from <https://www.thestar.com.my/news/nation/2018/09/23/fake-news-still-a-crime-in-malaysia-in-this-transition-period-where-rules-are-constantly-being-negot/>
- Verizon Enterprise. (2018). *Data Breach Investigations Report*. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
- Verizon. (2018). 2018 data breach investigations report (11th ed.). Retrieved from <http://www.verizonenterprise.com/>
- Vermesan, O., & Friess, P. (2014). *Internet of Things – From Research and Innovation to Market Deployment*. Aalborg: River Publishers.
- Verplanken, B., & Holland, R. W. (2002). Motivated Decision Making: Effects of Activation and Self-Centrality of Values on Choices and Behavior. *Journal of Personality and Social Psychology*, 82(3), 434–447. doi:10.1037/0022-3514.82.3.434 PMID:11902626
- Viano, E. C. (2017). Cybercrime: Definition, Typology and Criminalization. In E. C. Viano (Ed.), *Cybercrime, Organized Crime and Societal Response*. Washington, DC: Springer Press. doi:10.1007/978-3-319-44501-4_1
- Viber. (2018). *Free and secure calls and messages to anyone, anywhere*. Retrieved from <https://www.viber.com/>
- Vilà, J. A. (2015). Identifying and combating cyber-threats in the field of online banking. Barcelona: Academic Press.
- Villacampa, C., & Gómez, M. J. (2017). Online child sexual grooming: Empirical findings on victimisation and perspectives on legal requirements. *International Review of Victimology*, 23(2), 105–121. doi:10.1177/0269758016682585

Vinagre, M. (2008). Politeness strategies in collaborative e-mail exchanges. *Computers & Education*, 50(3), 1022–1036. doi:10.1016/j.compedu.2006.10.002

Vincent, D. (2011, May). China used prisoners in lucrative Internet gaming work. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2011/may/25/china-prisoners-internet-gaming-scam>

Virginia, A. M. (2005). *Introduction to sociology of education*. Lagos: DMMM Publishers.

Vishwanath, A. (2016, May 5). Cybersecurity's weakest link: humans. *The Conversation*. Retrieved from <https://theconversation.com/cybersecuritys-weakest-link-humans-57455>

Vishwanath, A. (2016). Spear phishing: The tip of the spear used by cyber terrorists. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 469–484). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0156-5.ch023

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4), 451–470. doi:10.1080/08838151.2012.732140

Vlachos, A., & Riedel, S. (2014). Fact Cheching: task definition and dataset construction. *Proceedings of the ACL Workshop on Language Technologies and Computational Social Science*, 18-22. 10.3115/v1/W14-2508

Vogel, K. P., & Benner, K. (2019, April 12). Ex-Obama Aide Indicted in Case Linked to Mueller Report. *New York Times*, p. A16.

Vogeley, K. (2013). A Social Cognitive Perspective on 'Understanding' and 'Explaining'. *Psychopathology*, 46(5), 295-300. doi:10.1159/000351839

Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007, February). Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. *NDSS*.

Von Ahn, L. (2003). *CAPTCHA: Using Hard AI Problems for Security*. Springer Berlin Heidelberg.

Voronova, S., & Radjenovic, A. (2016). *The Gender Dimension of Human Trafficking*. European Parliamentary Research Service (EPRS). PE 577.950. Retrieved December 4, 2018 from [http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI\(2016\)577950_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI(2016)577950_EN.pdf)

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Nature*, 359(6380), 1146–1151. PMID:29590045

Voss, K. (2016). Plausibly Deniable: Mercenaries in US Covert Interventions During the Cold War, 1964-1987. *Cold War History*, 16(1), 37–60. doi:10.1080/14682745.2015.1078312

Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2017). The dark side of working online : Towards a definition and an Emotion Reaction model of workplace cyberbullying. *Computers in Human Behavior*, 69, 324–334. doi:10.1016/j.chb.2016.12.055

Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2018). When workplace bullying goes online: Construction and validation of the Inventory of Cyberbullying Acts at Work (ICA-W). *European Journal of Work and Organizational Psychology*, 27(1), 28–39. doi:10.1080/1359432X.2017.1363185

Vulcan Post. (2017). *5 Challenges FavePay & Other Cashless Wallets Must Overcome To Grow In M'sia*. Retrieved from <https://vulcanpost.com/620539/challenges-ewallet-cashless-malaysia/>

Wada, F., Longe, O., & Danquah, P. (2012). Action speaks louder than words-understanding cyber criminal behavior using criminological theories. *Journal of Internet Banking and Commerce*, 17(1), 1–12.

Compilation of References

- Wade, A., & Beran, T. (2011). Cyberbullying: The new era of bullying. *Canadian Journal of School Psychology*, 26(1), 44–61. doi:10.1177/0829573510396318
- Wagner, L. I., Duffecy, J., Penedo, F., Mohr, D. C., & Cella, D. (2017). Coping strategies tailored to the management of fear of recurrence and adaptation for E-health delivery: The FoRtitude intervention: Managing Fear of Recurrence. *Cancer*, 123(6), 906–910. doi:10.1002/cncr.30602 PMID:28207157
- Wagstaff, K. (2012, March 6). You'd need 76 work days to read all your privacy policies each year. *Time*. Retrieved from <http://techland.time.com/2012/03/06/you-d-need-76-work-days-to-read-all-your-privacy-policies-each-year/>
- Wahab, O. A., Bentahar, J., Otok, H., & Mourad, A. (2017). Optimal Load Distribution of VM-based DDoS Attacks in the Cloud. *IEEE Transactions on Services Computing*.
- Wakabayashi, D. (2018, June 28). California passes major online privacy law. *The New York Times*, p. B1.
- Wakefield, J. (2019, 16 march). Christchurch shootings: Social media races to stop attack footage. *BBC*. Retrieved from <https://www.bbc.com/news/technology-47583393>
- Walker, J. (2017, November 13). AI chatbot used to combat phishing by wasting scammers' time. *Digital Journal*. Retrieved from <http://www.digitaljournal.com/tech-and-science/technology/ai-chatbot-used-to-combat-phishing-by-wasting-scammers-time/article/507506>
- Walker, S. (2016). *Online abuse: how different countries deal with it*. Retrieved 12th of November 2018 from <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>
- Walker, K. (2016). Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection. *Journal of Public Policy & Marketing*, 35(1), 144–158. doi:10.1509/jppm.15.020
- Walker, M., & Townly, C. (2012). Contract cheating: A new challenge for academic honesty? *Journal of Academic Ethics*, 10(1), 27–44. doi:10.1007/10805-012-9150-y
- Walker, S. (2012). Economics and the cyber challenge. *Information Security Technical Report*, 17(1-2), 9–18. doi:10.1016/j.istr.2011.12.003
- Wall, D. (2007). *Cybercrime: the Transformation of Crime in the Information Age*. Academic Press.
- Wall, D. D. S. (2002). *Crime and the Internet*. London: Routledge.
- Wall, D. S. (2005). The internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 77-98). Thousand Oaks, CA: Sage Publications. doi:10.4135/9781452225708.n4
- Wallace, M. J., & Newton, P. M. (2014). Turnaround time and market capacity in contract cheating. *Educational Studies*, 40(2), 233–236. doi:10.1080/03055698.2014.889597
- Wallarm. (2018, Nov 19). *Wallarm New Open Source Module and Kaggle Hackathon*. Retrieved from <https://lab.wallarm.com/wallarm-new-open-source-module-and-kaggle-hackathon-8ce0824a967e>
- Wall, D. (2001). *Crimes and the Internet: Cybercrimes and Cyberfears*. London: Routledge Press. doi:10.4324/9780203164501
- Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
- Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers & Technology*, 22(1–2), 45–63. doi:10.1080/13600860801924907

- Wall, D. S. (2008/11). Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime (revised Feb. 2011). *Information Communication and Society*, 11(6), 861–884. doi:10.1080/13691180802007788
- Walsh, P. F., & Miller, S. (2016). Rethinking ‘Five Eyes’ security intelligence collection policies and practice post Snowden. *Intelligence and National Security*, 31(3), 345–368. doi:10.1080/02684527.2014.998436
- Walsh, T. (2018). *Machines That Think: The Future of Artificial Intelligence*. Amherst, MA: Prometheus Books.
- Waltz, E. L. (1998). *Information warfare principles and operations*. Artech House, Inc.
- Wang, H., Philpot, A., Hovy, E. H., & Latonero, M. (2014). *Data Mining and Integration to Combat Child Trafficking*. Retrieved from Carnegie Mellon University, School of Computer Science website: <http://www.cs.cmu.edu/~hovy/papers/12dgo-trafficking.pdf>
- Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information*, 6(2), 183–211. doi:10.3390/info6020183
- Wang, P., Wang, X., Wu, Y., Xie, X., Wang, X., Zhao, F., ... Lei, L. (2018). Social networking sites addiction and adolescent depression: A moderated mediation model of rumination and self-esteem. *Personality and Individual Differences*, 127, 162–167. doi:10.1016/j.paid.2018.02.008
- Wang, Y. S., Wang, Y. M., Lin, H. H., & Tang, T. I. (2003). Determinants of user acceptance of Internet banking: An empirical study. *International Journal of Service Industry Management*, 14(5), 501–519. doi:10.1108/09564230310500192
- Ward, A. (2019, August 12). A Norwegian white nationalist tried to kill Muslims at a mosque. *Vox*. Retrieved from <https://www.vox.com/2019/8/12/20801735/norway-mosque-attack-el-paso-muslims>
- Wardle, C. (2017). *Fake News. It's Complicated*. Retrieved from <https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79>
- Wardle, C. (2017, February 16). *Fake news. It's complicated*. Retrieved January 23, 2018, from First Draft News website: <https://firstdraftnews.com/443/fake-news-complicated/>
- Ward, T., & Siegert, R. (2002). Toward a comprehensive theory of child sexual abuse: A theory of knitting perspective. *Psychology, Crime & Law*, 8(4), 319–351. doi:10.1080/10683160208401823
- Warman v Kyburz, (2003 CHRT 18) (2003/05/09) para. 81.
- Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, 5(1), 736.
- Warner-Soderholm, G., Bertsch, A., Sawe, E., Lee, D., Wolfe, T., Meyer, J., ... Fatilua, U. (2018). Who trusts social media? *Computers in Human Behavior*, 81, 303–315. doi:10.1016/j.chb.2017.12.026
- Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. doi:10.2307/1321160
- Wash, R., & Cooper, M. M. (2018). Who provides phishing training? Facts, stories, and people like me. CHI 2018, Montréal, Canada. Doi:10.1145/3173574.3174066
- Washburn, K. (2018). *Violence Against Women Act at risk of lapsing*. Retrieved 12th of November 2018 from <https://www.opensecrets.org/news/2018/10/vawa-at-risk-of-lapsing/>
- Washington, V., DeSalvo, K., Mostashari, F., & Blumenthal, D. (2017). The HITECH Era and the Path Forward. *The New England Journal of Medicine*, 377(10), 904–906. doi:10.1056/NEJMp1703370 PMID:28877013

Compilation of References

- Wasserman, T. (2018, March 21). *Chatbots Are All the Rage—and Something of a Risk*. Retrieved from <https://www.securityroundtable.org/chatbots-rage-something-risk/>
- Watkin, W. (2019). *What we learned from Cambridge Analytica*. Retrieved from <https://www.brunel.ac.uk/news-and-events/news/articles/What-we-learned-from-Cambridge-Analytica>
- Watson, H. J. (2014). Tutorial: Big Data Analytics: Concepts, Technologies, and Applications. *Communications of the Association for Information Systems*, 34, 65. doi:10.17705/1CAIS.03465
- Wayman. (2005). An Introduction to Biometric Authentication Systems. *Biometric Systems*, 1-20.
- Wazid, M. (2013). A framework for detection and prevention of novel keylogger spyware attacks. *2013 7th International Conference on Intelligent Systems and Control (ISCO)*. 10.1109/ISCO.2013.6481194
- We Are Social Singapore. (2017, January). *Digital in 2017: Southeast Asia*. Internet. Retrieved from <https://www.slideshare.net/wearesocialsg/digital-in-2017-southeast-asia>
- We Are Social. (2019). *Digital 2019 Global Digital Overview*. Available at <https://www.slideshare.net/DataReportal/digital-2019-global-digital-overview-january-2019-v01>
- Weatherbee, T. G. (2006). A case of cyberdeviancy : Cyberaggression in the workplace Human Resource Management Review Counterproductive use of technology at work : Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, 20(1), 35–44. doi:10.1016/j.hrmr.2009.03.012
- Webb, G. (2018). *Whistle-blowers and research fraud – we should reward not shoot the messenger*. Retrieved from <https://drgeoffnutrition.wordpress.com/2018/07/15/whistleblowers-and-research-fraud-dont-shoot-the-messenger/>
- Webb, T. J. (2011), Verbal Poison-Criminating Hate Speech: A Comparative Analyse and a Proposal for the American System. *Washburn L.J.*, 50.
- Webber, C., Yip, M. (2018). The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. *International Journal of Cyber Criminology*, 230-254.
- Weber, B. (1996, February 18). It's Man Over Machine as Chess Champion Beats Computer He Calls Tough Opponent. *New York Times*.
- Weber, M. (2000). *Sosyoloji Yazıları*. İstanbul: İletişim Yayınları.
- Weber, S. H., & Studer, E. (2016). Cybersecurity in the internet of things: Legal aspects. *Computer Law & Security Review*, 32(5), 715–728. doi:10.1016/j.clsr.2016.07.002
- Weber-Wulff, D. (2014). False feathers: A perspective on academic plagiarism. Berlin, Germany: Springer Science+Business Media. doi:10.1007/978-3-642-39961-9
- Webroot. (2017). *Phishing Attacks Growing in Scale and Sophistication*. Retrieved from https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf
- Weckert, J. (2000). *Computer ethics: future directions*. Retrieved November 13, 2018, from <http://www.acs.org.au/act/events/2000acs4.html>
- Wedgbury, A., & Jones, K. (2015). Automated Asset Discovery in Industrial Control Systems - Exploring the Problem. *3rd International Symposium for ICS & SCADA Cyber Security Research*. 10.14236/ewic/ICS2015.8
- Weedon, J., Nuland, W., & Stamos, A. (2017). *Information Operations and Facebook*. Facebook Security.

- Wegberg, R. v., Oerlemans, J.-J., & Deventer, O. v. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419–435. doi:10.1108/JFC-11-2016-0067
- Weimann, G. (2004). *How modern terrorism uses the Internet. Special Report No.116*. United States Institute of Peace. Retrieved from www.terror.net
- Weimann, G. (2016). Going dark: Terrorism on the dark Web. *Studies in Conflict and Terrorism*, 39(3), 195–206. doi:10.1080/1057610X.2015.1119546
- Weimann, G. (2016). Terrorist migration to the dark web. *Perspectives on Terrorism*, 10(3).
- Weinberg, D. B., & Pehlivan, E. (2015). Social spending: Managing the Social Media Mix. *Business Horizons: Kelly School of Business*, 54(3), 275–282. doi:10.1016/j.bushor.2011.01.008
- Weiner, R., & Hawkins, D. (2018, June). Hackers stole federal workers' information four years ago. Now we know what criminals did with it. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/public-safety/hackers-stole-feds-information-four-years-ago-now-we-know-what-criminals-did-with-it/2018/06/19/f42ff2b2-73d3-11e8-805c-4b67019fcfe4_story.html?utm_term=.f41861167c0f
- Weinstein, L. (2003). Spam wars. *Communications of the ACM*, 46(8), 136. doi:10.1145/859670.859703
- Welcome to DuckDuckGo. (n.d.). Retrieved from <https://duckduckgo.com/about>
- WeLiveSecurity. (2015, July). The 6 biggest online gaming hacks. *WeLiveSecurity.com*. Retrieved from <https://www.welivesecurity.com/2015/07/02/6-biggest-online-gaming-hacks/>
- West, B., Foster, M., Levin, A., Edmison, J., & Robibero, D. (2014). Cyberbullying at Work : In Search of Effective Guidance. *Technology, Social Media and Laws*, 3(3), 598–617. doi:10.3390/laws3030598
- WestJ. (2014). *Cybercrime against women*. Retrieved from <http://www.bwss.org/wp-content/uploads/2014/05/Cyber-VAWReportJessicaWest.pdf>
- What is the HITECH ACT? | What HITECH Compliance Means. (2009). Retrieved from <https://compliance-group.com/what-is-the-hitech-act/>
- What is the Offence of Contempt of Court in Singapore? (2018, November 2). Retrieved from SingaporeLegalAdvice.com website: <https://singaporelegaladvice.com/law-articles/contempt-of-court-singapore>
- What is TOR? (n.d.). Retrieved from <https://www.eff.org/torchallenge/what-is-tor.html>
- what-is-ssl.html. (n.d.). Retrieved from <https://www.sslshopper.com/what-is-ssl.html>
- WhatsApp. (2018). *Simple. Secure. Reliable messaging*. Retrieved from <https://www.whatsapp.com/>
- Wheeler, T. (2017). How the Republicans Sold Your Privacy to Internet Providers. *New York Times*. Retrieved March 29, 2017 from <https://www.nytimes.com/2017/03/29/how-the-republicans-sold-your-privacy-to-internet-providers.html>
- Wheeler, T. (2017, March 28). The G.O.P. just sold your privacy. *The New York Times*, p. A27.
- White, J. S., Matthews, J. N., & Stacy, J. L. (2012). *A method for the automated detection phishing websites through both site characteristics and image analysis* (Vol. 8408). doi:10.1117/12.918956
- Whitman, M. E., & Mattord, H. J. (2019). *Management of information security* (6th ed.). Boston, MA: Cengage.

Compilation of References

- Whitney, J., Jennex, M., Elkins, A., & Frost, E. (2018). *Don't Want to Get Caught? Don't Say It: The Use of EMOJIS in Online Human Sex Trafficking Ads*. Academic Press.
- Whittaker, E., & Kowalski, R. M. (2015). *Cyberbullying Via Social Media*. Taylor & Francis.
- Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior, 18*(1), 62–70. doi:10.1016/j.avb.2012.09.003
- Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665–684. doi:10.1093/bjc/azt009
- Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking, 15*(3), 181–183. doi:10.1089/cyber.2011.0352 PMID:22304401
- Whitty, M. T., Doodson, J., Creese, S., & Hodges, D. (2017). A picture tells a thousand words: What Facebook and Twitter images convey about our personality. *Personality and Individual Differences*; Advance online publication. doi:10.1016/j.paid.2016.12.050
- Wierzbicki, A. (2018). *Web Content Credibility*. Springer. doi:10.1007/978-3-319-77794-8
- Wiki/computer crime. (2006). *Computer crime*. Retrieved December 3, 2018, from http://en.wikipedia.org/wiki/computer_crime
- Wilcox, H., Bhattacharya, M. & R. Islam. (2014). Social Engineering through Social Media: A comprehensive investigation on enterprise security. *Applications and Techniques in Information Security, Communications in Computer and Information Science, 243-255*.
- Wilford, H. (2017). American Friends of the Middle East: The CIA, US Citizens, and the Secret Battle for American Public Opinion in the Arab-Israeli Conflict, 1947-1967. *Journal of American Studies, 51*(1), 93–116. doi:10.1017/S0021875815001255
- Willard, N. (2005). *Cyberbullying and Cyberthreats*. Center for Safe and Responsible Use of the Internet.
- Williams, J. A. (2008). *Counterfeiting of goods: The risks and links to terrorist funding*. Retrieved from <http://www.osi.com.ph/wp-content/uploads/Counterfeiting-Links-to-Terrorist-Funding-Article.pdf>
- Williams, M. (2006). *Virtually Criminal: Crime, Deviance and Regulation Online*. Routledge.
- Williams, M. L. (2015). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology, 56*(1), 21–48. doi:10.1093/bjc/azv011
- Williams, S. L., & French, D. P. (2011). What are the most effective intervention techniques for changing physical activity self-efficacy and physical activity behaviour—And are they the same? *Health Education Research, 26*(2), 308–322. doi:10.1093/her/cyr005 PMID:21321008
- Willsher, K., & Henley, J. (2017). *Emmanuel Macron's campaign hacked on eve of French election*. Retrieved from <https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election>
- Wilmot, S. (2000). Nurses and whistleblowing: The ethical issues. *Journal of Advanced Nursing, 32*(5), 1051–1057.
- Wilson, C. (2008). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service – Report for Congress. Retrieved December 3, 2018, from <https://fas.org/sgp/crs/terror/RL32114.pdf>
- Wilson, A. (2005). *Virtual politics: faking democracy in the post-Soviet world*. Yale University Press.

- Windrem, R. (2016). *Timeline: Ten Years of Russian Cyber Attacks on Other Nations*. Retrieved from <https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111>
- Winkelman, S. B., Early, J. O., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring Cyber harassment among women who use social media. *Universal Journal of Public Health*, 3(5), 194-201.
- Winker, M. A., Flanagan, A., Chi-Lum, B., White, J., Andrews, K., Kennett, R. L., ... Musacchio, R. A. (2000). Guidelines for Medical and Health Information Sites on the Internet: Principles Governing AMA Web Sites. *Journal of the American Medical Association*, 283(12), 1600–1606. doi:10.1001/jama.283.12.1600 PMID:10735398
- Wireless Application Forum. (2001). *Wireless Transport Layer Security*. Wireless Application Protocol WAP-261-WTLS-20010406-a, Version 06.
- Withrow, S. C. (2010). How to avoid a HIPAA horror story: The HITECH Act has expanded the financial risk for hospitals that do not meet the privacy and security requirements under HIPAA. *Healthcare Financial Management*, 64(8), 82–89. PMID:20707266
- Witmer, B. G., & Singer, M. J. (1998). Measuring presence in virtual environments: A presence questionnaire. *Presence (Cambridge, Mass.)*, 7(3), 225–240. doi:10.1162/105474698565686
- Witting, S. (2017, June). ‘Cyber’ Trafficking? An Interpretation of the Palermo Protocol in the Digital Era. *Völkerrechtsblog*, 28. doi:10.17176/20170629-162348
- Wolak, J., Finkelhor, D., & Mitchell, K. (2012). Trends in Arrests for Child Pornography Possession: The Third National Juvenile Online Victimization Study (NJOV-3). *Crimes Against Children Research Center*. Retrieved from <https://scholars.unh.edu/ccrc/46>
- Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online “Predators” and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. *The American Psychologist*, 63(2), 111. <http://dx.doi.org.ezaccess.libraries.psu.edu/10.1037/0003-066X.63.2.111>
- Wolak, J., Evans, L., Nguyen, S., & Hines, D. A. (2013). Online Predators: Myth versus Reality. *New England Journal of Public Policy*, 25(1), 1–11.
- Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *The Journal of Adolescent Health*, 41(6), S51–S58. doi:10.1016/j.jadohealth.2007.08.019 PMID:18047945
- Wolfgang, M. E., Thornberry, T. P., & Figlio, R. M. (1987). *From Boy to Man, from Delinquency to Crime*. Chicago, IL: University of Chicago Press.
- Wolford, B. (2018, August 27). What is the dark web? The good and bad of the Internet’s most private corner. *Proton-Mail*. Retrieved from <https://protonmail.com/blog/what-is-dark-web/>
- Wombat Security. (2015). The Cost of Phishing & Value of Employee Training. Retrieved from <https://www.wombat-security.com/cost-of-phishing>
- Wombat Security. (2016). The State of the Phish. Retrieved from <https://www.wombatsecurity.com/state-of-the-phish>
- Wong, D. S., Chan, H. C. O., & Cheng, C. H. (2014). Cyberbullying perpetration and victimization among adolescents in Hong Kong. *Children and Youth Services Review*, 36, 133–140. doi:10.1016/j.childyouth.2013.11.006

Compilation of References

- Wong, R. C.-W., Li, J., Fu, A. W.-C., & Wang, K. (2006). (α , k)-anonymity: an enhanced k -anonymity model for privacy preserving data publishing. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 754–759). ACM.
- Wood, A. K. (2017, October). *Show Me the Money: "Dark Money" and the Informational Benefit of Campaign Finance Disclosure*. University of Southern California Legal Studies Working Paper Series. Working Paper 254. Retrieved from <http://law.bepress.com/usclwps-lss/254>
- Wood, J. A. (2009). The darknet: A digital copyright revolution. *Rich. JL & Tech.*, 16, 1.
- Working Group on Intimate Partner Abuse and Relationship. (2002). Intimate partner abuse and relationship violence. *American Psychological Association*. Retrieved from <https://www.apa.org/about/division/activities/partner-abuse.pdf>
- World Economic Forum. (2018). *The Global Risks Report 2018*. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf
- World Health Organization. (2010). *World Health Report, 2010: Health Systems Financing – the path to universal coverage*. Geneva: WHO. Retrieved from https://www.who.int/whr/2010/10_summary_en.pdf
- Wright, M. F. (2013). The relationship between young adults' beliefs about anonymity and subsequent cyber aggression. *Cyberpsychology, Behavior, and Social Networking*, 16(12), 858–862. doi:10.1089/cyber.2013.0009 PMID:23849002
- Wright, M. F. (2015). Cyber victimization and adjustment difficulties: The mediation of Chinese and American adolescents' digital technology usage. *Cyberpsychology (Brno)*, 1(1), 1. Retrieved from <http://cyberpsychology.eu/view.php?cisloclanku=2015051102&article=1>
- Wright, M. F., Kamble, S., Lei, K., Li, Z., Aoyama, I., & Shruti, S. (2015). Peer attachment and cyberbullying involvement among Chinese, Indian, and Japanese adolescents. *Societies (Basel, Switzerland)*, 5(2), 339–353. doi:10.3390/soc5020339
- Wright, M. F., & Li, Y. (2012). Kicking the digital dog: A longitudinal investigation of young adults' victimization and cyber-displaced aggression. *Cyberpsychology, Behavior, and Social Networking*, 15(9), 448–454. doi:10.1089/cyber.2012.0061 PMID:22974350
- Wright, T. (2010). The Stoke CNEP Saga - how it damaged all involved. *Journal of the Royal Society of Medicine*, 103(7), 277–282. doi:10.1258/jrsm.2010.10k012 PMID:20406828
- Wright, V. H., Burnham, J. J., Inman, C. T., & Ogorchock, H. N. (2009). Cyberbullying: Using Virtual Scenarios to Educate and Raise Awareness. *Journal of Computing in Teacher Education*, 26(1), 35–41.
- Wu, J., & Yang, G. (2005). An ontology-based method for project and domain expert matching. In L. Wang, & Y. Jin (Eds.), *Fuzzy systems and knowledge discovery* (vol. 3614, pp. 176–185). Berlin: Springer. doi:10.1007/11540007_22
- Wurmser, Y. (2018, June 18). Mobile time spent 2018. *eMarketer*. Retrieved from <https://www.emarketer.com/content/mobile-time-spent-2018>
- Wurzinger, P., Bilge, L., Holz, T., Goebel, J., Kruegel, C., & Kirda, E. (2009). Automatically Generating Models for Botnet Detection. *LNCS*, 5789, 232–249. doi:10.1007/978-3-642-04444-1_15
- Wu, T. (2018). Is the First Amendment obsolete? *Michigan Law Review*, 117(3), 547–581.
- Wynn, D., & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *Management Information Systems Quarterly*, 36(3), 787–810. doi:10.2307/41703481
- Xenakis, C., & Ntantogian, C. (2014). An advanced persistent threat in 3g networks: Attacking the home network from roaming networks. *Computers & Security*, 40, 84–94. doi:10.1016/j.cose.2013.11.006

- Xiao, B. S., Chan, T. K. H., Cheung, C. M. K., & Wong, R. Y. M. (2016). An Investigation into Cyberbullying perpetration: a routine Activity Perspective. *PACIS*, 370.
- Xing, J., & Sieber, R. E. (2018). Propagation of Uncertainty for Volunteered Geographic Information in Machine Learning (Short Paper). In *10th International Conference on Geographic Information Science (GIScience 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
- Yahoo, Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme, et al 145 F. Supp. 2d 1168, Case No. C-00-21275JF (N.D. Ca., September 24, 2001).
- Yang, J., Ma, H., Song, W., Cui, J., & Zhou, C. (2006). Crawling the edonkey network. In *2006 fifth international conference on grid and cooperative computing workshops* (pp. 133–136). 10.1109/GCCW.2006.29
- Yang, J. H. (2016). Social media analytics for intelligence and countering violent extremism. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 328–348). Hershey, PA: IGI Global.
- Yang, K., & Lee, H. J. (2010). Gender differences in using mobile data services: Utilitarian and hedonic value approaches. *Journal of Research in Interactive Marketing*, 4(2), 142–156. doi:10.1108/17505931011051678
- Yang, Y., & Nenkova, A. (2017, September). Combining lexical and syntactic features for detecting content-dense texts in news. *Journal of Artificial Intelligence Research*, 60(1), 179–219. doi:10.1613/jair.5418
- Yang, Y., Wilson, L. T., & Wang, J. (2010). Development of an automated climatic data scraping, filtering and display system. *Computers and Electronics in Agriculture*, 71(1), 77–87. doi:10.1016/j.compag.2009.12.006
- Yang, Y., Wu, L., Yin, L., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250–1258. doi:10.1109/JIOT.2017.2694844
- Yanisky-Ravid, S. (2014). To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory. *American University Law Review*, 5(64), 53–108. Retrieved September 19, 2018 from <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1939&context=aulr>
- Yan, X., Song, D., & Li, X. (2006, November). Concept-based document readability in domain specific information retrieval. In *Proceedings of the 15th ACM international conference on Information and knowledge management* (pp. 540–549). ACM. 10.1145/1183614.1183692
- Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407–427. doi:10.1177/147737080556056
- Yar, M. (2013). *Cybercrime and Society*. Thousand Oaks, CA: SAGE Publications.
- Ybarra, M. L., Diener-West, M., & Leaf, P. (2007). Examining the overlap in internet harassment and school bullying: Implications for school intervention. *The Journal of Adolescent Health*, 1(6), 42–50. doi:10.1016/j.jadohealth.2007.09.004 PMID:18047944
- Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, 45(7), 1308–1316. doi:10.1111/j.1469-7610.2004.00328.x PMID:15335350
- Yeargain, J. W., Settoon, R. P., & McKay, S. E. (2004). Can-Spam Act of 2003: How to spam legally. *Journal of Strategic E-Commerce*, 2(1), 15–30.

Compilation of References

- Yegneswaran, V., Giffin, J. T., Barford, P., & Jha, S. (2005). An architecture for generating semantic-aware signatures. *USENIX Security Symposium*.
- Yen, I. (2008). Of vice and men: A new approach to eradicating sex trafficking by reducing male demand through educational programs and abolitionist legislation. *The Journal of Criminal Law & Criminology*, 98(2), 653–686.
- Yilmaz, H. (2011). Cyberbullying in Turkish middle schools: An exploratory study. *School Psychology International*, 32(6), 645–654. doi:10.1177/0143034311410262
- Ying, H., Maglaras, L., Janicke, H., & Jones, K. (2015). An Industrial Control Systems incident response decision framework. *IEEE Conference on Communications and Network Security*. 10.1109/CNS.2015.7346923
- Yin, R. (2017). *Case Study Research and Applications: Design and Methods*. Thousand Oaks, CA: Sage Publications.
- Yong, P. (2011). *New China Criminal Legislations in the Progress of Harmonization New China Criminal Legislations in the Progress of Harmonization*. Retrieved November 29, 2018, from <https://rm.coe.int/16803042f0>
- Young, K. S. (2011). Clinical assessment of Internet-addicted clients. In K. S. Young & C. N. de Abreu (Eds.), *Internet addiction: A handbook and guide to evaluation and treatment* (pp. 19–34). Hoboken, NJ: John Wiley & Sons Inc.
- Yousef, W. S. M., & Bellamy, A. (2015). The impact of cyberbullying on the self-esteem and academic functioning of Arab American middle and high school students. *Electronic Journal of Research in Educational Psychology*, 23(3), 463–482.
- YouTube. (2018). *Best of YouTube*. Retrieved from <https://www.youtube.com/>
- Yu, J. (2018). *Chinese cyber attacks on Taiwan government becoming harder to detect: source*. Retrieved from <https://www.reuters.com/article/us-taiwan-china-cybersecurity/chinese-cyberattacks-on-taiwan-government-becoming-harder-to-detect-source-idUSKBN1JB17L>
- Yu, S. (2011). Email spam and the CAN-SPAM Act. *International Journal of Cyber Criminology*, 5(1), 715–735.
- Yu, S. (2014). Sex in Spam. *International Journal of Criminal Justice Sciences*, 9(1), 35–45.
- Yu, S., Guo, S., & Stojmenovic, I. (2015). Fool me if you can: Mimicking attacks and anti-attacks in cyberspace. *Computers. IEEE Transactions on*, 64(1), 139–151.
- Zaidenberg, N. J. (2018). Hardware Rooted Security in Industry 4.0 Systems. *Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures*, 51, 135–151.
- Zaidenberg, N., Neittaanmäki, P., Kiperberg, M., & Resh, A. (2015). Trusted Computing and DRM. In *Cyber Security: Analytics, Technology and Automation* (pp. 205–212). Cham: Springer. doi:10.1007/978-3-319-18302-2_13
- Zaitsev, D. (2018). Sleptsov Net Computing. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (4th ed.; pp. 7731–7743). Hershey, PA: IGI Global. Doi:10.4018/978-1-5225-2255-3.ch672
- Zaitsev, D. A. (2019). Sleptsov Net Computing. In M. Khosrow-Pour, D.B.A. (Ed.), *Advanced Methodologies and Technologies in Network Architecture, Mobile Computing, and Data Analytics* (pp. 1660–1674). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7598-6.ch122
- Zarifis, A., Cheng, X., Dimitriou, S., & Efthymiou, L. (2015). *Trust in Digital Currency Enabled Transactions Model*. MCIS.
- Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C., & Vigna, G. (2014, November). The dark alleys of madison avenue: Understanding malicious advertisements. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (pp. 373–380). ACM. 10.1145/2663716.2663719

- Zastrow, C. (2013). *Sosyal Hizmeti Giriş*. Ankara: Nika Yayınevi.
- Zetter, K. (2017, June 3). *Tor Hires a New Leader to Help It Combat the War on Privacy*. Retrieved from <https://www.wired.com/2015/12/tor-hires-a-new-leader-to-help-it-combat-the-war-on-privacy/>
- Zhang, J., Lee, G., & Wang, J. (2016). *A Comparative Analysis of Univariate Time Series Methods for Estimating and Forecasting Daily Spam in United States*. Academic Press.
- Zhang, J., Perdisci, R., Lee, W., Luo, X., & Sarfraz, U. (2014). Building a scalable system for stealthy P2P-botnet detection. *Information Forensics and Security, IEEE Transactions on*, 9(1), 27–38.
- Zhang, C., Dhungel, P., Wu, D., Liu, Z., & Ross, K. W. (2010, March). *Bittorrent darknets*. In *2010 proceedings IEEE infocom* (pp. 1–9). IEEE. doi:10.1109/INFCOM.2010.546196
- Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., . . . Yue, C. (2016). The highly insidious extreme phishing attacks. *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, 1–10. 10.1109/ICCCN.2016.7568582
- Zhao, G., Xu, K., Xu, L., & Wu, B. (2015). Detecting apt malware infections based on malicious dns and trac analysis. *IEEE Access: Practical Innovations, Open Solutions*, 3, 1132–1142. doi:10.1109/ACCESS.2015.2458581
- Zhong, Y., & Deng, Y. (2015). *Recent Advances in User Authentication Using Keystroke Dynamics*. Science Gate Publishing. DOI: . doi:10.15579/gcsr.vol2.ch4
- Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*. Retrieved 2018, October 3, from <https://arxiv.org/ftp/arxiv/papers/1802/1802.03110.pdf>
- Zhou, Y. (2018, May 25). An Oregon family's encounter with Amazon Alexa exposes the privacy problem of smart home devices. *Quartz*. Retrieved from <https://qz.com/1288743/amazon-alexa-echo-spying-on-users-raises-a-data-privacy-problem/>
- Zhou, L., Ding, L., & Finin, T. (2011). How is the Semantic Web evolving? A Dynamic Social Network Perspective. *Computers in Human Behavior*, 27(4), 1294–1302. doi:10.1016/j.chb.2010.07.024
- Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, 26(4), 760–767. doi:10.1016/j.chb.2010.01.013
- Zhou, Z., Tang, H., Tian, Y., Wei, H., Zhang, F., & Morrison, C. M. (2013). Cyberbullying and its risk factors among Chinese high school students. *School Psychology International*, 34(6), 630–647. doi:10.1177/0143034313479692
- Zicari, P. (2008). *Students admit lying, cheating, stealing to ethics survey*. Retrieved from https://www.cleveland.com/nation/index.ssf/2008/12/students_admit_lying_cheating_.html
- Ziegeldorf, J., Morchon, O., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728–2742. doi:10.1002/ec.795
- Zimba, A., Wang, Z., Mulenge, M., & Odongo, N. H. (2018). Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. *Journal of Computer Information Systems*.
- Zimmerman, A. G. (2012). *Online Aggression: The Influences of Anonymity and Social Modelling*. University of North Florida. Retrieved 12th of November 2018 from <https://digitalcommons.unf.edu/cgi/viewcontent.cgi?article=1472&context=etd>
- Zimmerman, C., & Kiss, L. (2017). Human trafficking and exploitation: A global health concern. *PLoS Medicine*, 14(11), e1002437. doi:10.1371/journal.pmed.1002437 PMID:29166396

Compilation of References

- Zlomislic, V., Fertalj, K., & Sruk, V. (2014). Denial of service attacks: an overview. *Proceedings of the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6.
- Zolkipli, M. F., & Jantan, A. (2011). An approach for malware behavior identification and classification. *Computer Research and Development (ICCRD), 2011 3rd International Conference*.
- Zolkipli, M. F., & Jantan, A. (2010). Malware Behavior Analysis: Learning and Understanding Current Malware Threats. *2010 Second International Conference on Network Applications, Protocols and Services*. 10.1109/NETAPPS.2010.46
- Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9), 1727–1765. doi:10.1109/JPROC.2016.2558521
- Zulkefli, Z., Mahinderjit-Singh, M., & Malim, N. (2015). Advanced Persistent Threat Mitigation Using Multi Level Security Access Control Framework. *Lecture Notes in Computer Science*, 9158, 90–105. doi:10.1007/978-3-319-21410-8_7
- Zurkus, K. (2018, September 14). Microsoft Office Macros Still No. 1 Malware Delivery. Retrieved from <https://www.infosecurity-magazine.com/news/microsoft-office-macros-still-no-1/>

About the Contributors

Mehdi Khosrow-Pour, D.B.A., received his Doctorate in Business Administration from the Nova Southeastern University (Florida, USA). Dr. Khosrow-Pour taught undergraduate and graduate information system courses at the Pennsylvania State University – Harrisburg for almost 20 years. He is currently Executive Editor at IGI Global (www.igi-global.com). He also serves as Executive Director of the Information Resources Management Association (IRMA) (www.irma-international.org) and Executive Director of the World Forgotten Children Foundation (www.worldforgottenchildren.org). He is the author/editor of more than 100 books in information technology management. He is also currently the Editor-in-Chief of the *International Journal of E-Politics (IJEP)* and the *International Journal of Semiotics and Visual Rhetoric (IJSVR)*, and is also the founding Editor-in-Chief of the *Information Resources Management Journal (IRMJ)*, *Journal of Electronic Commerce in Organizations (JECO)*, *Journal of Cases on Information Technology (JCIT)*, and the *Journal of Information Technology Research (JITR)*, and has authored more than 50 articles published in various conference proceedings and scholarly journals.

* * *

Fernando Luís Almeida has a PhD in Computer Science Engineering from Faculty of Engineering of University of Porto (FEUP). He also holds an MSc in Innovation and Entrepreneurship and an MSc in Informatics Engineering from FEUP. He has around 8 years of teaching experience at higher education levels in the field of computer science and management. He has also worked for 15 years in several positions as software engineer and project manager for large organizations and research centers like Critical Software, CICA/SEF, INESC TEC and ISR Porto. During that time, he had the chance to work in partnership with big international organizations and universities in several European projects. His current research areas include innovation policies, entrepreneurship, software development and cyber security.

Bede Ravindra Amarasekara is currently pursuing his PhD at Massey University in New Zealand. Having spent many years in the industry as a Software Developer, his current research interests are in web-based technologies.

Athanasios Anastasiou received his Bachelor degree in Electrical & Electronic Engineering from the University of Newcastle Upon Tyne, in 2005. In 2006, he received his M.Sc. degree in Digital Signal & Image Processing from the University of Central Lancashire. Likewise, in 2009 he obtained his second M.Sc. degree in Biomedical Engineering held by the University of Patras and the National Technical University of Athens (N.T.U.A.). In 2015, received his PhD degree in Biomedical engineering in the field

About the Contributors

of mobile health. Since 2011, he is a member of the Biomedical Engineering Laboratory of N.T.U.A.. His current research interests comprise Bioinformatics, Biosignal Processing, Digital Image Processing and technologies for assisted living. He is a Member of the Institute of Electrical and Electronics Engineers (IEEE) - EMBS Society and Computer Society, Member of the Institution of Engineering and Technology (IET) and a member of the Technical Chamber of Greece (TEE).

Thelma Androutsou is a PhD Candidate at Biomedical Engineering Laboratory, National Technical University of Athens.

Christopher Anglim works at both the University of the District of Columbia and the Washington College of Law at American University. He has a longstanding interest in the areas of Constitutional Law, Legislation, Jurisprudence, Cyber Law, and Privacy Law. He has written several books and articles, including a major encyclopedia on privacy law.

Fardaus Ara graduated in Public Administration from Dhaka University, Bangladesh. She did her MPhil from Bergen University, Norway and PhD from Murdoch University, WA. She joined Bangladesh Palli Karma Sahayak Foundation, an apex micro-finance organization, as a deputy manager in 1996. She is serving Rajshahi University as an academic since 1998.

Sandal Azhar has completed her graduation in Physical Science (Electronics) from Andc, University of Delhi and also holds a Post graduate degree in Electronics from Jamia Millia Islamia. She is currently pursuing Post Graduate Diploma in Cyber Security and Law from Institute of Cyber Security and Law, University of Delhi.

Antonio Badia is the author of more than 50 peer-reviewed papers and the recipient of several NSF research grants, including the prestigious CAREER Award. He is also the author of “The Information Manifold”, forthcoming from MIT Press. At the University of Louisville, he founded and directs the Database Research Lab.

Liudmila Baeva is Full Professor, Doctor of Philosophy, Dean of the Department of Social Communication, Professor of the Chair of Philosophy of Astrakhan State University. Author of over 220 articles and 6 monographs. Research interests focus on the field of axiology, philosophical anthropology, and the study of the information society issues. A member of the editorial board of the international journal “Socioloska luca: Journal of Social Anthropology, Social Demography & Social Psychology” (Montenegro) and the editorial board of the international journal “The Caspian Region: Economics, Politics and Culture” (Russia). Visiting Professor of Philosophy at Moscow State Technical University (Russia, 2005), Hainan University (China, 2007), South Kazakhstan State University named after M. Auezov, (City of Shymkent, Kazakhstan, 2011). Participated in the World Congresses of Philosophy in Istanbul, Seoul, and Athens.

Leroy Baldwin is an associate professor of Criminal Justice at Atlanta Metropolitan State College in Atlanta, Georgia, USA. He received a B.S. in Political Science from Florida A&M University and the Doctor of Jurisprudence degree from John Marshall Law School. In addition to having practiced law, he has also served as a high school teacher and has been published in Who’s Who Among America’s Teachers four times.

Aakash Bali is B.Tech Student at JayPee University of Information Technology, Solan, India.

Himani Bansal is B.Tech Student at Jaypee University, Solan, India.

Simone Barbato is a Clinical Psychologist. Graduated in Clinical Psychology with the thesis: “Digital psychology as a support for the person”, he specialized in “Human Performance Psychology” in Turin. He earned a Master in “Human Resources Management and Administration”, with the thesis “Virtual Reality and Employer Branding: from innovation to new selection standard”. He is Co-founder of IDEGO - Digital Psychology and Professor of Sport Psychology at University of Cassino.

Nii Barnor Jonathan Barnor is doctoral researcher in the University of Ghana Business School. He has a masters degree in management information systems and a bachelors degree in linguistics and music. His research interests are cybercrime, information systems security, information systems adoption, ICT for development, digital mobile maps and digital technologies.

Maria Basdeki is a lawyer, member of the Chalkida Bar Association, currently working for the Greek NGO Allilengyie/SolidarityNow in Athens, Greece. The main objective of work is providing assistance to vulnerable groups of people and participating in advocacy schemes for supporting their rights.

Punam Bedi is a Professor in the Department of Computer Science, University of Delhi since March 2007. She worked as officiating Director, Delhi University Computer Centre from Oct. 20, 2017 to April 16, 2018. She was the Head of Department of Computer Science, University of Delhi during Oct. 2005 - Oct 2008. She also worked as the acting Director, Delhi University Computer Centre from June 26 to Oct. 23, 2009. Before joining the Department of Computer Science, University of Delhi, she worked as a Lecturer/ Reader in the Deshbandhu College, University of Delhi from January 1987 to January 2002. She did her Doctorate in Computer Science from University of Delhi in 1999. She did her M.Tech. in Computer Science from IIT Delhi in 1986 and M.Sc. in Mathematics from IIT Delhi in 1984. She is mainly working in the area of designing and developing intelligent systems. She is using multi agent systems for the development of Intelligent Systems. Fuzzy Logic, Trust and Web Mining are the main techniques used for personalization of these systems based on users’ interests.

Monica Bell is a Neuroscience & Behavioral Studies and Philosophy major from the University of Notre Dame class of 2019.

Vladlena Benson is a Professor of Information Systems at Aston Business School. She is a specialist in technology governance, risk and compliance (GRC) and a Government Communications Headquarters (GCHQ)-certified Cyber Security Risk Management Frameworks practitioner. She is currently working with UK businesses on privacy and cyber security initiatives, such as the forthcoming General Data Protection Regulation (GDPR) and privacy compliance. Prof Benson’s research areas cover: information privacy; cyber victimisation; gender and culture differences in online behaviour; digital rights and the cyber vulnerability of young people. Her work also relates to religious orientation, digital behaviour and privacy on social media. She is a strong advocate for increasing diversity in the cyber security work force, and actively endeavours to bring more female talent into the digital economy. As part of her research, she currently runs a number of projects to help target the digital skills crisis – developing tools

About the Contributors

for opening up cyberspace entrepreneurship opportunities from an early age. As a result of her work in this area, Prof Benson was recognised at the Women in IT Awards 2017 for helping the development of career opportunities for women in cyber security.

Richard Boateng is an Associate Professor of Information Systems at the University of Ghana Business School. Richard's research experience covers digital economy, e-business, internet banking and social media. His papers have been published in or are forthcoming in the International Journal of Information Management, Internet Research, Qualitative Market Research: An International Journal, and many others.

Roman Brandtweiner is professor at the University of Economics and Business Vienna. His main research interests lie in the field of technology and society and green IT issues.

Frederick Edem Broni Jnr holds an MPhil degree in Management Information Systems and also a Teaching Assistant at the Operations and Management Information Systems Department (OMIS), University of Ghana Business School (UGBS). His background is in Computer Science and Management. His research interests are in Blockchain, Cryptocurrencies, Cloud Computing, Online Security and Privacy, and E-learning.

Joshua E. Byrd is a native of Atlanta, Georgia, USA. His professional career includes work as a criminal justice subject matter expert and staff attorney for a multinational litigation company. He currently serves as a Program Chair and Professor of Criminal Justice at American Intercontinental University. He is a former deputy sheriff and an eight-year U.S. Marine Corps veteran. His research interests include, cybercrime, the school-to-prison pipeline, environmental justice and crime prevention through environmental design. He obtained his Bachelor of Science in Criminal Justice from Georgia State University, his Master of Science in Criminal Justice from the University of Cincinnati and his Doctor of Jurisprudence from North Carolina Central University, School of Law.

Muhammed Can holds BA in Economics from Selcuk University (Turkey), MA in International Relations from Swansea University (UK), PGCert in International Affairs from King's College London (UK) and Advanced Certificate in Terrorism Studies from University of St. Andrews (UK). Currently, he is a PhD candidate at University of Minho (Portugal) in Political Science and International Relations. His research interests comprise Artificial Intelligence, Hybrid Warfare, Chinese Foreign Policy, Emerging Technologies, the US-China relations.

Chiam Chooi Chea obtained Bachelor Economics (Honours), Masters in Business Administration (MBA) and PhD (Economics) in 2001, 2003 and 2014 respectively. Since early 2003, she started her lecturing in an international private university college and private university in Malaysia with a total academic experience of approximately 13 years. Her field of research interest is in the field of resource economics and the trend of open distance learning (ODL). She is currently affiliated with Open University Malaysia under OUM Business School based in Bangi Learning Centre, Selangor.

Xingyu Chen is a Behavioural Sciences Research Analyst at the Home Team Behavioural Sciences Centre. Chen's research is in the areas of resilience, safety and security psychology which is supplemented by his background in communications. He has researched the psychological factors driving the spread of information during situations of high uncertainty such as scares and conflicts. As a Behavioural Sciences Research Analyst, Chen has presented to Home Team officers, community leaders, and Home Team psychologists on a variety of topics such as fake news and resilience to terror attacks. He has also presented about resilience on the day after terror incidents at Safety, Security Watch Group (SSWG) seminars to institutes of higher learning as well as industry partners. His current research interests include online misinformation, social resilience, individual crisis preparedness, and sentiment analysis.

Vassilia Costarides has graduated from National Technical University of Athens, from the school of Mining and Metallurgical Engineering with a specialization in Materials Engineering. She proceeded her studies in Biomedical Engineering and has worked in the medical device industry for 6 years as a technical specialist. Since 2013 she has been participating in projects regarding public health, medical device nomenclature, health technology assessment and medical device technical specifications. Among her interests is also quality in health care and she is an ISO9001:2008 and ISO13485:2003 auditor. She is currently a PhD candidate in Biomedical Engineering in the National Technical University of Athens and a member of the Biomedical Engineering Lab and Applied Informatics in m-Health research team. She is also a member of the Technical Chamber of Greece.

Charles Crowell is a professor in the Department of Psychology. He also directs the Computing & Digital Technologies Program, an information technology-related minor in the College of Arts & Letters. Along with his empirical and theoretical work on basic mechanisms of learning and motivation, Prof. Crowell has been involved for some time in applications of psychology and technology to learning, productivity, and performance improvement in organizations. As part of this work, he has investigated how technology can be used to augment human performance in various learning and work settings. Prof. Crowell oversees the eMotion and eCognition lab at Notre Dame that is devoted to investigating a spectrum of psychological phenomena ranging from the basic mechanisms underlying human movement and imitation to the ways in which humans interact with and are influenced by modern technological tools and devices.

Boaventura DaCosta holds a Ph.D. in instructional technology, an M.A. in instructional technology/media, instructional systems, and a B.S in computer science from the University of Central Florida. His research is interdisciplinary, concentrated in the fields of computer science and instructional design, with a special interest in games and learning.

László Dornfeld finished law school at the University of Miskolc in 2015 with a cum laude degree. He won two first prizes at the National Conference of Scientific Students' Associations before graduation. He started his PhD after that, researching the topic of cybercrime investigation under the supervision of Prof. Dr. Erika Róth. He worked for the National Bureau of Investigation's Department of Cybercrime as a scientific intern for six months in 2016. He joined a Hercule III project at the University financed by EU's OLAF in 2018 about the criminal law protection of the EU's financial interests, researching the topic of money laundering in cyberspace. He finished his PhD course in 2018 and since then he is a

About the Contributors

doctoral candidate. In 2019, he joined the government agency Ferenc Mádl Institute of Comparative Law as a researcher. He is an organizing member of the PhD Section of the Hungarian Society of Criminology.

Ramanujam Elangovan has received his M.E. from Anna University, Chennai, Tamil Nadu. He is pursuing his research in the area of biomedical engineering. His current area of interests are Data Mining, Time Series Mining and Biomedical processing. He has also published papers in national and international conferences and journals.

Aaron C. Elkins is an Assistant Professor in the department of Management Information Systems and Director of the SDSU Artificial Intelligence Lab. His research focuses on developing AI models that fuse physiological and behavioral sensor data to predict human emotion and deception. Elkins conducts experiments investigating automated deception detection in the laboratory, borders, and airports. Complementary to the development of advanced AI systems is their impact on the people using them to make decisions. He also investigates how human decision makers are psychologically affected by, use, perceive, and incorporate the next generation technologies into their lives.

Verity Er is a Behavioural Sciences Research Analyst at the Home Team Behavioural Sciences Centre under the Ministry of Home Affairs Singapore. Together with a team of researchers, Verity explores how crises, such as violent extremist attacks, can adversely impact social cohesion. She is also a trainer for Home Team officers on how to handle race and religious issues in the workplace, and has presented at HTBSC's workshop on fake news. Verity is currently pursuing an MSc in Applied Psychology.

Julie Exposito is founder and CEO of Musicology Studio where she has developed an adaptive learning system based on students' learning and cognitive styles. She has implemented successful sequential programs with a focus on skill and experiential based curriculum design to serve diverse students of all ages and individuals with varying exceptionalities and special needs. Dr. Exposito has served as the English language program coordinator for the Florida Association of International Educators and on the faculty at Miami Dade College and Broward College, teaching English for Academic Purposes with a focus on language acquisition and international conflict resolution in a classroom of linguistically and culturally diverse adult learners. Dr. Exposito completed a Doctor of Education with a concentration in Higher Education Leadership and Organizational Leadership from Nova Southeastern University and a Master's in TESOL from Florida International University. She received a Bachelor of Science in Education and French from Skidmore College. Dr. Exposito continues to write articles on education, higher education, the international student, learning styles, academic integrity, academic writing, leadership, and organizational stress.

Leyla Gamidullaeva graduated from Penza State University, the Faculty of Economics and Management, getting qualifications of an economist. L. Gamidullaeva got her PhD in Economics from Penza State University of Architecture and Construction in 2010 followed by the title of associate professor in 2018. Now she is associate professor at the department of management and economic security of Penza State University. Currently, L. Gamidullaeva is doing her doctoral research in the regional innovation system management at St Petersburg State University. She has authored more than 200 refereed publications and over ten books in innovation management, regional economic growth, networking and collaboration.

Suraj Gangwar has done Masters in Mathematics from National Institute of Technology, Jalandhar. He is currently pursuing Post Graduate Diploma in Cyber Security and Law from the University of Delhi. He is a technology enthusiast. His interest lies in cybersecurity and cryptography.

Giulia Gargaglione has a Master Degree in Well-Being Psychology from Catholic University of Milan. She currently works as a consultant. Her approach is based on positive psychology, that is, the scientific study of optimal human functioning and flourishing. Instead of drawing on a “disease model” of human behavior, it focuses on factors that enable individuals and communities to thrive and build the best in life. Her main professional focus is on Psychology applied to new technologies. In particular, her main area of intervention regards technology adoption. Other areas of intervention pertain change management, IT consulting and training, HR learning and development.

Dimitra Giannouli is a Software Developer and has been member of the Computer Solutions SA's Research & Development Department since 2018. She has graduated from the Department of Digital Systems of the University of Piraeus, specializing in Development of Digital Services. During her Bachelor studies, she focused her research efforts on e-Health and Mobile Health sector and she participated in the research and implementation of innovative Mobile Health mechanisms powered by 5G Network Slicing.

Anteneh T. Girma received a PhD degree from Howard University in Computer Science /Cyber Security. He has also received his M.Sc. degree in Systems and Computer Science from Howard University, and he received his B.Sc. degree in Mathematics from Addis Ababa University. He has many years of cyber security consultancy and teaching experience, and served as the Director of Information Technology at Howard University. Currently, Dr. Anteneh T. Girma is an Associate Professor of Cybersecurity and Forensics at Robert Morris University. His research interests are in the area of Cybersecurity and Information Assurance, Cloud Computing and Security, Digital Forensics, IOT Analytics and Security, Cryptography, and Machine Learning. He is also currently serving as a technical reviewer of research papers on different Cybersecurity tracks for major annual international conference in information technology. Among the awards he had received include the best research paper of the conference award on international information technology conference and recognition award for outstanding research and academic achievement.

Pamela Goh is a Behavioural Sciences Research Analyst with the Home Team Behavioural Sciences Centre (HTBSC). As a research analyst, her individual research portfolio is encapsulated by the resilience theme, and it includes crowd psychology and cyber hygiene. In essence, she is interested in understanding what contributes to the individual, community, and national's resilience in the event of a crisis from these perspectives. A key research area that Pamela looks into is the role of non-governmental organisations in the event of a violent extremist attack, and how civil societies in general can contribute to and complement Singapore's governmental efforts. Together with her team in HTBSC, the other areas that she has looked into are Singaporeans' perceptions to national resilience, cyber resilience, and fake news. Apart from resilience, Pamela is also interested in and has helped to write research papers that are terrorism-related. In addition to research, she also conducts seminars and trainings for government stakeholders, community leaders, and private companies. Pamela also holds other appointments in HTBSC, including being an internship manager for HTBSC's internship programme, as well as a Victim

About the Contributors

Care Officer (VCO) under the Singapore Police Force. She is currently doing her Ph.D at the Nanyang Technological University.

Dylas Gudoshava studied Library and Information Science. Area of specialism includes Information Service Provision in the fields of Law, Health, Humanities and Social Sciences; Research and Publication; as well as Marketing of Information Products and Services.

Daya Sagar Gupta received his Ph.D. in Computer Science and Engineering and M. Tech in Computer Application with distinction from Indian Institute of Technology (ISM), Dhanbad, Jharkhand, India. He received his B. Tech in Computer Science and Engineering from UPTU Lucknow (UP), India. He is currently working as an assistant professor in the department of Computer Science and Engineering, Shershah College of Engineering Sasaram, Bihar, India. His research interest includes Information Security, Lattice-based Constructions and Cyber Security.

Neha Gupta is a research scholar at Department of Computer Science, University of Delhi. She completed her MCA (Masters in Computer Application) from Department of Computer Science, University of Delhi in 2017 and later did 6 months internship at Proptiger Realty Pvt Ltd in analytics and search engine optimization. Before her post-graduation, she did her BSc. (Computer Science) from Keshav Mahavidyalaya, University of Delhi in 2014.

Laura Pinto Hansen received her Ph.D. from University of California Riverside where within her degree in sociology, she specialized in criminology and large-scale organizations. Her primary research interests have included white collar financial crimes, having had an earlier career within the taxes and financial planning fields. Her current research is focused on cybercrime. With a sabbatical planned in 2020, she is planning to explore emergency management and responses to cybercrime and attacks.

Richard Herschel is a Professor in the Department of Decision & System Sciences Department at Saint Joseph's University. This department offers programs in Business Intelligence & Analytics at both the undergraduate and graduate levels. Before becoming an educator, Dr. Herschel worked at Maryland National Bank, Schering-Plough Corporation, Johnson & Johnson, and Columbia Pictures as a systems analyst. Dr. Herschel has researched and written extensively about knowledge management and business intelligence. He is the founding Editor of the International Journal of Business Intelligence Research and he served as the Educational Channel Expert for b-eye-network.com.

Bogdan Hoanca is a Professor of Management Information Systems at the University of Alaska Anchorage. Before joining UAA, Prof. Hoanca co-founded, started up and sold a company that builds components for fiber optic communications. He also helped start and consulted with a number of other start-up companies in optical fiber communications. Bogdan received a PhD in Electrical Engineering from the University of Southern California in 1999, an MS in Electrical Engineering from Syracuse University and an Electronics Engineer degree from the Polytechnic Institute of Bucharest, Romania. His current research interests revolve around information security and societal implications of technology.

Rumenigue Hohemberger is a Lecturer at the Federal Institute of Science, Education and Technology Farroupilha (IFFar, Alegrete, RS, Brazil). He holds BS degree in Computer Science from the

Federal University of Pampa (UNIPAMPA, Brazil, 2011) and Specialization (2017) in Computer Networks. Cisco Certified Network Associate (CCNA) Instructor. His primary research interests include IoT networking and security.

Edith Huber is a senior researcher at the Danube University Krems. Her research focuses on Cyber Security, CERTs, Information Security, Communication, Cybercrime, Cyberstalking, New Media, Social Science and Criminology.

Marisa Hultgren holds a Master of Science in Homeland Security from San Diego State University and a Bachelor of Arts in History and Geography with a concentration in Geographic Information Systems from California State University, Stanislaus. The main context of her research has been that of counter sex trafficking with an emphasis on the detection of victims through text mining of online data. She currently works in Southeast Asia in the humanitarian field of education to support at risk communities in impoverished, rural villages.

Farida Jaha is a PhD student at the LTI laboratory at ENSA El Jadida, Chouaib Doukkali University. He does his research in the field of computer security and more precisely access control of the BYOD environment.

Helge Janicke is the Head of School of Computer Science and Informatics at De Montfort University, UK. His interests are covering formal verification techniques and their application to Cyber Security, SCADA and Industrial Control System Security as well as aspects of Cyber Warfare. He is working closely with Airbus Group and established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security and Forensics Research in 2013. He is a general chair of the International Symposium on SCADA and Industrial Control Systems Cyber Security Research (ICS-CSR) as well as serving on the editorial board and as reviewer of international journals.

Murray E. Jennex is a Professor of Management Information Systems at San Diego State University, editor-in-chief of the International Journal of Knowledge Management, co-editor-in-chief of IGI Global book series, co-editor-in chief of the International Journal of Information Systems for Crisis Response and Management, and President of the Foundation for Knowledge Management (LLC). Dr. Jennex specializes in knowledge management, crisis response, system analysis and design, IS security, e-commerce, and organizational effectiveness. Dr. Jennex serves as the Knowledge, Innovation, and Entrepreneurial Systems Track co-chair at the Hawaii International Conference on System Sciences. He is the author of over 150 journal articles, book chapters, and conference proceedings on knowledge management, crisis response, end user computing, international information systems, organizational memory systems, ecommerce, cyber security, and software outsourcing. Dr. Jennex is a former US Navy Nuclear Power Propulsion officer and holds a B.A. in chemistry and physics from William Jewell College, an M.B.A. and an M.S. in software engineering from National University, an M.S. in telecommunications management and a Ph.D. in information systems from the Claremont Graduate University. Dr. Jennex is also a registered professional mechanical engineer in the state of California and a Certified Information Systems Security Professional (CISSP), a Certified Secure Software Lifecycle Professional (CSSLP), and a Project Management Professional (PMP).

About the Contributors

Vinita Jindal is an Assistant Professor in the Department of Computer Science, Keshav Mahavidyalaya, University of Delhi since August 2001. She was the Head of Department of Computer Science, Keshav Mahavidyalaya, University of Delhi from June 2017 till May 2019. Before joining the Department of Computer Science, Keshav Mahavidyalaya, University of Delhi, she worked as a Manager/ Sr. Faculty in the PCTI Ltd. from July 1999 to July 2001. She did her Doctorate in Computer Science from University of Delhi in 2018. She did her M.Phil. in Computer Science from Madurai Kamaraj University in 2007, MCA from IGNOU in 2000 and Bachelor in Mathematics from University of Delhi in 1997. She is mainly working in the area of Artificial Intelligence and Networks. Her area of interest includes dark web, deep learning, Adhoc networks, Recommender Systems, Intrusion Detection System, and Vehicular Adhoc networks to name a few.

Kevin Jones is Head of Cyber Security Architecture, Innovation and Scouting at Airbus. He holds a BSc in Computer Science and MSc in Distributed Systems Integration from De Montfort University, Leicester where he also obtained his PhD: A Trust Based Approach to Mobile Multi-Agent System Security in 2010. Kevin has many years of experience in consultancy to aid organisations in achieving accreditation to ISO27001 standard on Information Security Management. He is a recognised expert in Critical National Infrastructure security, SCADA security, and the protection of critical systems. He currently acts as an executive consultant to Airbus on matters of cyber security across multiple domains and platforms and works closely with government agencies on cyber security topics in addition to European programmes such as the “European Control System Security Incident Analysis Network” and the EU Cyber Security Public Private Partnership. He is a frequent public speaker on cyber security and the protection of critical national infrastructure, in addition to an advisor to numerous cyber security research programmes and events. He is a member of the BCS, IEEE, ISACA, and ISC2 and is accredited as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and ISO27001 Lead Auditor.

Mitch Kajzer is a graduate of the Indiana Law Enforcement Academy class 89-97 and has been in law enforcement since 1989. He holds an Associates Degree in Criminal Justice from Indiana University, a Bachelor's Degree in Psychology from Indiana University, and a Master's Degree in Cognitive Psychology from the University of Notre Dame. He currently works for the Office of the Prosecuting Attorney in St. Joseph County, IN as the Director of the St. Joseph County Cyber Crimes Unit and for the University of Notre Dame as an adjunct professor in the Computing & Digital Technologies Program. Mitch began his law enforcement career with the South Bend, Indiana Police Department. Over the course of his law enforcement career, he held a number of different positions, including road patrol, detective, and traffic crash reconstructionist. Mitch has instructed over 5000 police officers on a number of topics, including officer survival, police action shootings, critical incidents, emergency vehicle operation, accident investigation, computer forensics, technology crimes, Internet investigations, and undercover investigations. In his 30 years in law enforcement, Mitch has been involved in a number of critical incidents, including being shot in the line-of-duty. He has also been awarded the Police Purple Heart and in 1995 was inducted into the American Police Hall of Fame, Legion of Honor. Mitch has been investigating cybercrimes since 2003. He currently holds a number of computer industry technology certifications, including Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Professional with Internet Expertise (MCP+I), A+ Certified Computer Technician, Certified Internet Webmaster – Professional (CIW-P), Certified Computer Examiner (CCE), and Magnet Certified Fo-

rensis Examiner (MCFE). Moreover, Mitch has investigated over 2000 technology-related cases and has conducted over 2500 digital examinations, resulting in hundreds of arrests and convictions. In addition to his work at the Cyber Crimes Unit, Mitch is also an adjunct faculty member at the University of Notre Dame. He currently teaches three undergraduate courses; 1) Introduction to Digital Forensics, 2) Advanced Digital Forensics, and 3) Forensic Psychology – Threat Assessments. Moreover, he conducts research that focuses on constructing algorithms to be used in predictive text analysis on Internet communications of child sexual offenders. Mitch has authored multiple peer-reviewed journal publications and academic conference presentations, both domestic and international, related to the psychology and communications of Internet child sexual offenders. Finally, Mitch also works as a contract trainer for Magnet Forensics Corporation of Waterloo, Ontario. In this capacity, he teaches a number of digital analysis courses throughout the United States to law enforcement and the technology professionals. These include Forensic Fundamentals, IEF Examinations, AXIOM Examinations, Advanced Computer Examination, and Advanced Mobile Forensics.

Ali Kartit is a renowned researcher in the field of information system security at LTI laboratory at ENSA El Jadida. He is involved in research projects in fields related to security & mobility, artificial intelligence applied to security, healthcare & security and research in encrypted data. He is now a full professor at ENSA El Jadida- Chouaib Doukkali University.

Prabhjyot Kaur did B.Sc. Mathematics (Honors) from Jesus and Mary College, University of Delhi in 2015. She did M.Sc. Mathematics (Honors) from LSR College, University of Delhi in 2017. She has interned in Defence Research and Development Organisation for two months and worked on the topic “Cryptography and Cryptanalysis”. Ms Kaur is currently pursuing her one-year Post Graduate Diploma in Cyber Security and Law from University of Delhi.

Puneet Kumar Kaushal has completed his B.Tech and M.Tech in Computer Science and Engineering with specialization in Networks and Security. His research interest included blockchain, cryptocurrency, distributed ledger technology, and decentralized applications and & its security. He has experience of 6 years as Assistant Professor and presently delivering cyber security and cryptography trainings in multiple Universities in north India.

Mayank Kejriwal is a research lead at the University of Southern California’s Information Sciences Institute (ISI), and a research assistant professor in USC’s Department of Industrial and Systems Engineering. He received his Ph.D. from the University of Texas at Austin. His dissertation involved Web-scale data linking, and in addition to being published as a book, was recently recognized with an international Best Dissertation award in his field. His research is highly applied and sits at the intersection of knowledge graphs, social networks, Web semantics, network science, data integration and AI for social good. He has contributed to systems used by both DARPA and by law enforcement, and has active collaborations across academia and industry. He is currently co-authoring a textbook on knowledge graphs (MIT Press, 2018), and has delivered tutorials and demonstrations at numerous conferences and venues, including top academic venues such as KDD, AAAI, and ISWC, and industrial venues. He is currently serving as general chair of the ACM K-CAP conference in 2019, and is co-editing a special issue on knowledge graphs in the Semantic Web Journal. He was awarded a Key Scientific Challenges award in 2018 by the Allen Institute for Artificial Intelligence, and was recently named a Forbes Under 30 Scholar.

About the Contributors

Nasreen Khan is a senior lecturer in the Faculty of Management, Multimedia University, Malaysia. She received her PhD from University Malaya in 2012. She has been an academician for over ten years and was involved actively in teaching, research, and supervision. Her publications have appeared in various international refereed journals and conference proceedings. Her research interests include service marketing, technology marketing, marketing communication, consumer behavior and human resource management.

Shereen Khan is a Lecturer and Unit Coordinator at the Law Unit, Faculty of Management, Multimedia University. She obtained her LLB (Hons) Degree from the International Islamic University, Malaysia and completed Master in Comparative Laws from the same University and admitted as an advocate and solicitor at the High Court of Malaya. She obtained her Doctorate from the National University of Malaysia. Her area of research for the Ph.D was on the Company Law, in particular on corporate insolvency. Dr. Shereen Khan's main research interests are on Company Law, Business Law and Cyber Law. She lectures on Company Law, Business Law and Cyber Law at the Faculty.

Tehmina Khan is an academic at RMIT, School of Accounting, Melbourne, Australia. She has published widely in the area of sustainability (social and environmental) accounting and accountability.

Michael Kiperberg was born in Ukraine, in 1987, and migrated to Ashkelon, Israel. He received B.Sc. and M.Sc. degrees in Computer Sciences from the Tel Aviv University, Israel, in 2009 and 2012, and his Ph.D. degree from the University of Jyväskylä, Finland. Michael is currently holding a position of a lecturer at the Holon Institute of Technology (HIT), Israel. Michael's research interests include virtualization and security.

Marcos Paulo Konzen is a Lecturer at the Federal Institute of Science, Education and Technology Farroupilha (IFFar, Alegrete, RS, Brazil). He holds BS degree in Informatics from the Methodist College of Santa Maria (FAMES, Brazil, 2009), MSc (2012) degree in Production Engineering from the Federal University of Santa Maria (UFSM, Brazil). Cisco Certified Network Associate (CCNA) Instructor. His primary research interests include software-defined networking and network security.

Muhammet Köroğlu has been an Assistant Professor at Uşak University, Faculty of Economics and Administrative Sciences, Social Work Department. He obtained his Master's Degree from Selçuk University Philosophy and Religious Sciences Department in 2004. And he obtained his PhD from Necmettin Erbakan University in 2012. He focused on relations of public sphere and religion in his PhD researches. His research interests are social and religious movements, social work with elderly and relations of autonomous public spheres, and religion.

Ana Lambrecht is a lawyer. Investigator Institute of Public Politics and Government of the National University of Río Negro (UNRN).

Mufutau Lamidi is Professor of Generative Syntax and Contact Linguistics at the University of Ibadan, Nigeria. His research interests include Syntax, Contact Linguistics, Sociolinguistics, Applied Linguistics and Media Studies. He has written books and several journal articles which are published in reputable outlets locally and internationally.

Roe Leon finished his MSc in Software Engineering in JYU at 2016 and his PhD at 2019. Roe researches the field of applications of hypervisors in security.

Leandros A. Maglaras received the B.Sc. degree from Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from University of Thessaly in 2004, and M.Sc. and PhD degrees in Electrical & Computer Engineering from University of Volos, in 2008 and 2014 respectively. In 2018 he was awarded a PhD in Intrusion Detection in SCADA systems from University of Huddersfield. He is the head of the National Cyber Security Authority of Greece and a part time Senior-Lecturer in the School of Computer Science and Informatics at De Montfort University, U.K. He serves on the Editorial Board of several International peer-reviewed journals such as IEEE Access and Wiley Journal on Security & Communication Networks. He is an author of more than 90 papers in scientific magazines and conferences and is a senior member of IEEE.

Roberto Marmo received the Laurea (cum laude) in Computer Science from Salerno University (Italy) and Ph.D. in Electronic and Computer Engineering obtained from the University of Pavia (Italy). He is presently contract teacher of computer science at Faculty of Engineering of Pavia University, Italy. His most recent work is concerned with mathematical models and software for social network analysis. He is author of “Social Media Mining”, a textbook in Italian language on help extraction of business information from social media, website <http://www.socialmediamining.it>.

Anuradha Mathrani is a senior lecturer in Information Technology in the School of Natural and Computational Sciences at Massey University, Auckland, New Zealand. Her research interests include software quality and reliability measurements, distributed software architectures, application lifecycle management, technology enhanced teaching/learning practices and e-commerce governance methods.

Rande W. Matteson retired in 2006, as a Senior Supervisory Special Agent (Federal Agent) after a 32-year law enforcement career having served in responsible international and domestic leadership-management and field and special covert assignments. During his career, Matteson served in various special project assignments and as an Agency Commander at the 2001 Winter Olympics in Salt Lake City, UT. Matteson had diplomatic assignments in Latin America, the Middle East-Asia and domestically. He served in the Leadership Unit at the FBI-DEA Academy and HQTS as a Manager-Supervisory Special Agent. Matteson has been qualified as an expert witness in federal courts and is a subject matter expert (SME) in many varied aspects of crime. In addition, he is certified as a fraud examiner, hostage negotiator, and in maritime security and a physical fitness coordinator. He has completed numerous Marathons and international and domestic Ironman and Sprint distance triathlons. He is a faculty member at Nova Southeastern University serving as a doctoral dissertation mentor and teaches graduate courses in leadership. Previously, he served as an Associate Professor (Department Chair) in the Department of Criminal Justice Flagship Program. He developed and taught undergraduate and graduate classes in law, leadership, economic crime, budgeting, violent crime, terrorism, ethics, criminal investigation, and fiscal management. He holds membership in over 12 professional organizations and has participated-served on 25 various academic committees. He has authored over 25 scholarly publications, numerous textbook chapters, and several books. He frequently presented various subject matter topics at many domestic

About the Contributors

and international venues and faculty colloquiums. In addition to his scholarly publication record, he has served as an editor and on research committees for scholarly publications. His scholarly interests include complex global social and societal justice issues tied to dysfunctional leadership.

Anita W. McMurtry is an Assistant Professor of Criminal Justice at Atlanta Metropolitan State College. She holds a Ph.D. in Criminal Justice from Capella University, and M.A. in Criminal Justice from Clark Atlanta University. She teaches both face-to-face and online criminal justice courses at the undergraduate level. She also served as a Death Investigation Specialist at Georgia Bureau of Investigation for seven years. Her research interests are juvenile delinquency, juvenile corrections, service oriented programs for youth, and African American issues.

Maria Rosa Miccoli is an expert in Psychology for Well-Being and Behavioral Sciences. Graduated in Psychology for Well-Being with the thesis: “The role of Financial Literacy, trust in Politics and Personality in decision making behavior with effects on long term: a comparison between Italy and Germany” in Milan. She completed one year of internship in the field of behavioral sciences, attending it partially in IULM (Milan, Italy) and partly at the FHWS (Würzburg, Germany).

Vardan Mkrttchian received his Doctorate of Sciences (Engineering) in Control Systems from Lomonosov Moscow State University (former USSR). Dr. Vardan Mkrttchian taught for undergraduate and graduate student’s courses of control system, information sciences and technology, at the Astrakhan State University (Russian Federation), where he was is the Professor of the Information Systems (www.aspu.ru) six years. Now he is full professor in CAD department of Penza State University (www.pnzgu.ru). He is currently chief executive of HHH University, Australia and team leader of the international academics (www.hhhuniversity.com). He also serves as executive director of the HHH Technology Incorporation. Professor Vardan Mkrttchian has authored over 400 refereed publications. He is the author of over twenty books published of IGI Global, included ten books indexed of SCOPUS in IT, Control System, Digital Economy, and Education Technology. He is also has authored more than 200 articles published in various conference proceedings and journals.

Kenrick Mock is a Professor of Computer Science and has worked in the computing field since 1990. He is the author of several textbooks on computer programming, conducts research in intelligent systems, and has served as Associate Dean and Interim Dean for the University of Alaska Anchorage College of Engineering.

Anne-Marie Mohammed is a Lecturer in Economics at The University of the West Indies, St. Augustine, Trinidad and Tobago. She received her Ph.D. degree in Economics from The University of the West Indies, St. Augustine. Her current research interests include industrial economics, economics of regulations, crime and tourism and applied microeconomics.

Sovik Mukherjee is at present Assistant Professor, Department of Economics, Faculty of Commerce & Management Studies, St. Xavier’s University, Kolkata, India. Formerly, Senior Lecturer in Economics, Department of Commerce (Evening; UG & PG) at Shri Shikshayatan College, Kolkata, India. A research fellow in the Department of Economics, Jadavpur University, Kolkata, India. His research interests lie in the areas of applied game theory, applied growth econometrics, energy & environmental economics

and issues related to climate change, socio-health economics, and the econometric analysis of financial crises. He has been awarded with the MOTHER TERESA GOLD MEDAL AWARD_ 2017 for contributions in the field of Economic Growth Research by the Global Economic Progress and Research Association, New Delhi, India. He is a Life Member of the Indian Economic Association (IEA), The Indian Econometric Society (TIES) and the Bengal Economic Association (BEA).

Vinayak Narang has completed his graduation in BSc(H)Chemistry and is currently pursuing Post Graduate Diploma in Cyber Security and Law. He is a people's person who loves to interact with everyone.

Loo Seng Neo is a Principal Behavioural Sciences Research Analyst with the Home Team Behavioural Sciences Centre at the Ministry of Home Affairs, Singapore. For the past 12 years, Loo Seng has been specialising in the area of violent extremism, particularly in the fields of online radicalisation, online threat assessment, pre-attack warning signs, and psychology of violent extremism. He works with a team of research analysts undertaking behavioural sciences research on violent extremism, resilience and intergroup conflict. He has presented at many international conferences, trained law enforcement officers, and published many government research reports and peer-reviewed journals and book chapters on the topic of violent extremism. He has also co-edited a book titled 'Combating Violent Extremism and Radicalisation in the Digital Era' in 2016, and a four-volume compendium titled 'A Behavioural Sciences Approach to Understanding Terrorism' in 2017. Loo Seng is currently pursuing his PhD in psychology researching on the personality profile of violent extremists at Nanyang Technological University.

Eileen O'Donnell was conferred by Dublin City University with an Honours (2.1) BSc Degree in Information Technology and a First Class MSc in Information Systems for Managers. While lecturing on the Post Graduate Diploma in Business Information Systems in the Dublin Institute of Technology a research interest in Technology Enhanced Learning (TEL) commenced. This interest evolved into the pursuit of a PhD through research conducted with the Knowledge and Data Engineering Group, School of Computer Science & Statistics, College of Engineering, Trinity College Dublin, Ireland. Research interests include: cloud computing, virtualisation, green computing, the use of ICT in higher education, instructional design, e-learning, technology enhanced learning, personalised e-learning, user profiling, social networking sites, and human computer interaction.

Liam O'Donnell worked for ten years in the computing industry before commencing employment as a lecturer in the College of Business, Dublin Institute of Technology, Ireland. Liam has lectured in Information Systems for over twenty-five years. He also has responsibility for the management of the computer network for the College of Business. Liam received his BSc in Computer Applications from Dublin City University and his MSc in Computing from Sligo Institute of Technology. Liam's research interests include: Management Information Systems (MIS), Enterprise Information Systems (EIS), cloud technologies, virtualisation, computer networks, Perl and Java programming, fuzzy logic, expert systems, genetic algorithms, Type 1 Diabetes (T1D), social networking sites, instructional design, personalised e-learning, and technology enhanced learning.

Acheampong Owusu holds a PhD in Information Systems from Limkokwing University of Creative Technology, Cyberjaya, Malaysia. He is a Lecturer at the Operations and Management Information Systems (OMIS) Department at the University of Ghana Business School. His research interests include

About the Contributors

Business Intelligence (BI) Systems and Analytics, Technology Diffusion, Cloud Computing, and Ecommerce. Acheampong has published several research articles in peer-reviewed journals. He can be reached at aowusu@ug.edu.gh or owuach@hotmail.com.

Olusola Oyero is a researcher and an associate professor in the Department of Mass Communication, Covenant University, Ota, Ogun state, Nigeria. He has written several articles in international and national journal. He is currently the Head of Department, Mass Communication, Covenant University, Ota, Nigeria.

Suresh Palanimuthu completed PhD at Anna University, Chennai and currently working as a Professor in Galgotias University, Greater Noida, Uttar Pradesh. He has 17 years of teaching experience. He has published more than 25 international journals and contributed book chapters.

Raphael Phan holds the chair of security engineering at the Multimedia University (MMU), having served in British, Swiss & Australian universities prior to his current appointment. He is co-designer of the U.S. NIST SHA-3 finalist BLAKE and has been invited to serve in over 100 peer-reviewed security conferences since 2005. He was the Program Chair of Mycrypt 2016, and General Chair of Asiacrypt 2007 & Mycrypt 2005. He is also the Coordinating Editor of the IOS Press Series in Cryptology & Information Security, and is in the Editorial Board of the Cryptologia journal. He currently guest edits a special issue of the IEEE Transactions on Dependable & Secure Computing with focus on paradigm shifts in cryptographic engineering. Raphael's Erdős number is 2, and h-index at least 31.

Stavros Pitoglou received his BSc in Physics from the University of Patras, Greece in 2000. He currently holds the Chief Technical Officer position in Computer Solutions SA, being responsible for the company's Research and Development activities which include several internal research projects in the fields of Chronic Disease Monitoring, Machine Learning & Artificial Intelligence, Biosignals and Computer Vision & Image Processing. Since 2004 he participated as Project Director or Senior Project Manager in several large-scale projects in the fields of Health IT and Medical Informatics as well as Public Institutions Enterprise Resource Management. His research interests are focused on issues of machine learning and artificial intelligence applications in the healthcare domain, distributed networks and data security-privacy. In addition, he is a PhD candidate in the Biomedical Engineering Laboratory, School of Electrical and Computer Engineering of the National Technical University of Athens.

Bettina Pospisil received the M.A. degree in sociology from the University of Vienna. In 2015 she was Research Assistant with the Institute of Instructional and School Development at the University of Klagenfurt and at the Institute for Information Management and Control at the Vienna University of Economics and Business. Since 2017 she works as Junior Researcher in different KIRAS and FWF funded projects at the Faculty of Business and Globalization at the Danube University Krems. 2017 she and her colleague received the Innovation Award of the Danube University Krems for the project called "CERT-Kommunikation II". By now Bettina Pospisil is the co-author of different papers and presented academic lectures at criminological and technical conferences. Her research interest includes the topics Cybersecurity and Crime Studies.

Christophe Premat is an Associate Professor in French with a major specialization in Cultural Studies at Stockholm University. He is a member of the editorial board of the review *Sens Public*, an international web journal of social sciences. His current research focuses on the perception of participatory processes in the political discourse of French-speaking elites, the analysis of memory debates in France and discourse analysis. He recently published a book on the institutionalization of Francophonie organization (*Pour une généalogie critique de la Francophonie*, Stockholm University Press, 2018) and co-edited in 2015 a handbook on French-German relations, *Handwörterbuch der deutsch-französischen Beziehungen* (Nomos). He is part of the research project analyzing the political discourses in Romance-speaking countries (ROMPOL, Stockholm University) and the research project “Language and power” (*Språk och Makt*, Stockholm University).

Gerald Quirchmayr holds doctoral degrees in computer science and law from Johannes Kepler University in Linz (Austria) and currently is Professor in the Multimedia Systems Research Group of the Faculty of Computer Science at the University of Vienna. In 2001/2002 he held a Chair in Computer and Information Systems at the University of South Australia. He first joined the University of Vienna in 1993 from the Institute of Computer Science at Johannes Kepler University in Linz (Austria) where he had previously been teaching. In 1989/1990 he taught at the University of Hamburg (Germany). His wide international experience ranges from the participation in international teaching and research projects, very often UN- and EU-based, several research stays at universities and research centres in the US, Asia and EU Member States to extensive teaching in EU staff exchange programs in the United Kingdom, Sweden, Finland, Germany, Spain, and Greece, as well as teaching stays in the Czech Republic and Poland. International teaching and specialist missions include UN-coordinated activities in Egypt, Russia and the Republic of Korea. He has served as a member of program committees of many international conferences, chaired several of them, has contributed as reviewer to scientific journals and has also served on editorial boards. He is a member of the Austrian and German computer societies and a member of IFIP working groups. For his contributions to the international IT community he was received the IFIP Silver Core Award in 1995. His major research focus is on information systems in business and government with a special interest in security, applications, formal representations of decision making and legal issues. His publication record comprises approximately 150 peer reviewed papers plus several edited books and conference proceedings as well as nationally and internationally published project reports. In July 2002 he was appointed as Adjunct Professor at the School of Computer and Information Science of the University of South Australia. From January 2005 until January December 2010 he headed the Department of Distributed and Multimedia Systems, Faculty of Computer Science, at the University of Vienna and served as Vice Dean of the Faculty of Computer Science from October 2008 until October 2010. Since January 2011 he serves as deputy head of the Multimedia Systems Research Group group. In 2011 he was appointed as Deputy Director of the Doctoral Studies Programme Natural and Technical Sciences, served as the programs Director from October 2014 until October 2016 and since then again as Deputy Director until October 2018.

Parthasarathi Ramamoorthy received his B.Tech in Information Technology in 2014 under the Anna University, Chennai, India. After graduation, he worked as the System engineer In Tata Consultancy services for more than two and a half years. Currently, he is pursuing Post Graduate diploma in Cybersecurity and law under the Delhi University, India. His main area of focus is on the Issues related to Blockchain and its associated technologies.

About the Contributors

Shalini Ramdeo is a Researcher at The University of the West Indies, St Augustine. Her work focuses specifically on workplace bullying, and organisational justice, with interests in organizational behaviour and organizational development.

Juhani Rauhala is a Research Affiliate and PhD student of cybersecurity at the University of Jyväskylä. He has over ten years' experience in the telecommunications industry, including design and management roles. He has been awarded two patents related to cloud storage. Juhani is a designated Eur Ing by the Federation of European Engineers, and is a senior member of the IEEE. He earned a BScEE (1992) and an MScE (1996) from San Francisco State University. His research interests include the weaponization of ubiquitous technologies and technology abuse.

Tansif ur Rehman has a PhD in European Studies. He has also completed six different Masters in the respective field of Social Sciences, i.e., MA (Economics), MA (International Relations), MA (Philosophy), MA (Political Sc.), MA (Sociology), M.Sc. (Gender & Women Studies). Along with these degrees he has also been able to complete 56 Certification/Credit Courses, 11 Miscellaneous Diplomas, 08 Government of Pakistan Trainings, 04 Certification Courses and Diploma (Languages) - Deutsch, English, Italian, and Russian. He is a Commissioned Class-1 Gazetted Officer, currently appointed as the Head of Sociology department at a respective government institute in Karachi (Pakistan). He is also working on various projects along with working as a Teaching Associate at the Department of Criminology (University of Karachi). He has several publications and has over 18 years teaching as well as 12 years research experience.

Amit Resh was born in Haifa, Israel, in 1959. He received his BSc. in Computer-Engineering and MBA from the Technion, Israel Institute of Technology, in 1986 and 2001 respectively. In 2013 he received his MSc. from the University of Jyväskylä, Finland. In 2016 he received his PhD. from the University of Jyväskylä, Finland. He has more than 25 years of professional experience in hi-tech companies in Israel and the USA. He has previously worked as Program-Manager at Apple and as VP of R&D at Connect One, as well as other companies in the embedded-systems industry. Currently he is COO of TrulyProtect, a startup company developing trusted computing systems based on virtualization technology.

Michael Robinson is a cyber security research engineer at Airbus. As part of the architecture, innovation and scouting team he provides cyber expertise to the business and supports state of the art research into new and novel cyber security solutions. He holds a BSc in Computer Science, an MSc in Computer Security from De Montfort University (UK), and a BA in International Relations from Keele University (UK). He obtained his PhD in cyber security in 2017 from De Montfort University. His research interests include cyber warfare, cyber peacekeeping, cloud security and cyber security risk management.

Nathan J. Rodriguez, Ph.D., is an Assistant Professor in the Department of Communication at Weber State University.

David B. Ross, a professor at Nova Southeastern University, teaches doctoral level courses in educational, organizational, and higher educational leadership. Learning from many perspectives and philosophies from mentors while attending Northern Illinois University, the University of Alabama, and Florida Atlantic University, has assisted him in guiding students in the learning process. Dr. Ross

earned his Doctorate in Educational Leadership, Master of Justice Policy Management with an Executive Certificate in Public Management at Florida Atlantic University, and his Bachelor of Science Degree in Computer Science at Northern Illinois University. Dr. Ross regularly speaks at conferences and provides consultation and training in the areas of leadership and management, policy issues, critical thinking, team building, professional development, academic writing, education, and behavior management. He has written articles and book chapters on leadership, power, narcissism, organizational stress, academic integrity, plagiarism and fraud, entitlement, mobbing/bullying, Gerontechnology, policy development, professional development, and areas of homeland security. Dr. Ross is a co-editor of a book titled Higher Education Challenges for Migrant and Refugee Students in a Global World. Dr. Ross is a dissertation chair and a reviewer for the university's Institutional Review Board. Dr. Ross was named Professor of the Year 2015-2016 for the Abraham S. Fischler College of Education. Dr. Ross is a retired Criminal Investigator/Agent with extensive-applied supervisory and field operations experience involving complex federal, state, local, and international crime; covert-clandestine operative and worked with informants; smuggling, profiling and drug interdiction; public order crime; asset forfeiture, money laundering, and conspiracy; wire and mail fraud; development of evidence for use in sworn affidavits, arrest and search and seizure warrants, pen registers; public and political corruption, technical operations including wire-oral intercepts, high technical human, stationary and aircraft/marine surveillance; intelligence-led programs, and RICO Act crimes.

Fábio Diniz Rossi is a Lecturer at the Federal Institute of Science, Education and Technology Farroupilha (IFFar, Alegrete, RS, Brazil). He holds BS degree in Informatics from the University of the Region of Campanha (URCAMP, Brazil, 2000), MSc (2008) and PhD (2016) degrees in Computer Science from the Pontifical Catholic University of Rio Grande do Sul (PUCRS, Brazil). Cisco Certified Network Associate (CCNA) Instructor. His primary research interests include Fog computing and IoT networking.

Valentina Rotelli obtained a master's degree in Well-being Psychology from the Catholic University (Milan, Italy) and majored in Behavioural Economics and Neuromarketing by cooperating both with IESUM (European Institute of the Human Behaviour Study) and with Catholic University in Milan. She attended an internship at the Faculty of Behavioural and Social Sciences in the field of Health Psychology and Behaviour change and modification, working on a research about the value orientation on reducing the consumption of red and processed meat.

George Saridakis is a Professor of Small Business and Entrepreneurship at the Kent Business School, where he directs the Centre for Employment, Competitiveness and Growth. He is also an Honorary Professor at the University of the West Indies, St. Augustine, Trinidad and Tobago. He received his PhD in Economics from the Institute for Social and Economic Research (ISER) at the University of Essex in 2006.

Melissa T. Sasso is an Italian Canadian native who grew up in Montreal, Quebec. Dr. Sasso attained her Bachelor of Arts in Psychology at Florida International University where she graduated with Cum Laude. She received both her Master's of Science in Exceptional Student Education and Doctorate in Education with a concentration in Organizational leadership at Nova Southeastern University, where she graduated with a 4.0 GPA in both degrees. Dr. Sasso has several years experience working with exceptional students who suffer from disabilities from Pre-K to grade 5 and is still interested in remaining within the education field. She has written articles with her Dissertation chair, Dr. David B. Ross, which

About the Contributors

can be found in NSUWorks and has her published dissertation entitled *How Narcissists Cannot Hold an Organization Together: A Mixed Method Approach to a Fictitious Puzzle Factory* located in ProQuest, as well as an international published book chapter within the book, “Chronic stress and its effect on brain structure and connectivity” entitled, “The increase of how mass media coverage manipulates our minds.” Her dissertation received a Dr. Charles L. Faires distinction award. In addition, she is an article reviewer and has also commenced editing various works. Her research interests include stress, and she is a passionate researcher in the fields of toxic workplace environments, narcissistic leadership, as well as academic entitlement.

Chris Scogings is Academic Dean of Information Sciences at Massey University. He is a specialist computer programmer and has been involved in the development of many software applications in order to solve unusual problems. He is an enthusiastic teacher of computer programming and has received the Vice-Chancellor’s award for Excellence in Teaching. His main research interests include computer simulation, artificial life and agent-based modelling.

Walter Seboeck studies political science at the University of Vienna (Dr., Conflict Research) as well as studies at the Vienna University of Economics and Business (Economics), Alaska Pacific University (MBA, Telecommunications Management) and at the Danube University Krems (MAS, MSc, Telematics Management). Presently Assistant Professor of Security Studies. Since 2001 he is head of the Center for Infrastructure Security at Danube University Krems. From 2009 to 2015, he was Head of Department for E-Governance and responsible for the development and expansion of the Department. From 2011 to 2012, he was Founding Dean and responsible for the development, structuring and establishment of the Faculty of Business and Globalization. In all areas and organizational units he was responsible for, research activities and agendas were founded and sustainably developed. From 2011 to 2013, as interim Head of Department of Economics, he was responsible for renovation and restructuring of the Department of Economics as well as for the Department’s expansion by a research area. From 2010 to 2013 he was a member of the Academic Senate of the University. Within the Senate, he headed the committee for honors (for services to the University) and was a member of the Curricular Commission. Seboeck is publisher of the *Journal of E-Democracy and Open Government (JeDEM)* and publisher of the conference proceedings for the annual Security Conference Krems (SiKo). He is a lecturer on information security and change aspects in the Digital Economy at Lomonosov University in Moscow, Hebei Finance University and Xingtai University in China.

Jamie Segerson is currently working in the field of Speech-Language Pathology. She received her Master’s Degree in Speech-Language Pathology from Wayne State University in 2019. Before beginning her Master’s program, Jamie spent two years working as an AmeriCorps literacy tutor in Washington, DC. She graduated from the University of Notre Dame in 2014 with a BBA in Management Consulting and a secondary major in Psychology and is originally from Dearborn, Michigan.

Soonhwa Seok holds a Ph.D. in curriculum and instruction. Her research foci include assistive technology and the digital literacy of students with autism, intellectual, and developmental disabilities. She has conducted extensive research in the area of behavior interventions using single case design. Complementing her research interests, she serves as a reviewer for a number of journals, to include *Educational Technology Research and Development* and the *British Journal of Educational Technology*.

Manisha Shahi completed her B.Sc Physical Science (Computer Science) from Maitreyi College, University of Delhi. She is currently pursuing her Post Graduate Diploma in Cyber Security and Law from Institute of Cyber Security and Law, University of Delhi.

Murad Al Shibli Associate Professor, has completed his Ph.D. in 2006 from Concordia University in Canada. Working as the Head of Autonomous and Artificial Intelligent Systems at Abu Dhabi Polytechnic in UAE as well as the Project Manager of Joint Aviation Command Program (JAC). Holds more than 25 years of industrial and academic experience in Canada, Jordan and UAE, at Concordia University, German Jordanian University, American University of Sharjah, UAEU University, and Abu Dhabi Polytechnic affiliated with Institute of Applied Technology. Established new programs in AI, Autonomous Systems, Electromechanical Engineering Technology and Mechatronics Systems. Worked as the chair of the Mechatronics Program at German Jordanian University. Published more than 50 publications in international journals and conferences. Registered 6 provisional patents in USA, filed two non-provisional patents at US Patent Office, and having two patents have been approved by TAKAMUL in UAE. Active researcher in AI systems, neural networks, machine learning and big data, robotics, autonomous systems, drones, anti-drone systems, control systems, mechatronics, space systems, and technical education paradigm.

Valentina Silvestri is a PhD Student in Experimental Psychology, Linguistics and Cognitive Neuroscience at University of Milano Bicocca (Milan, Italy) and Teaching Assistant in Developmental Psychology (head of the course: Professor Viola Macchi Cassia) at University of Milano Bicocca. Her research interests focus on emotion processing in infants. In particular, in understanding what could be the developmental trajectory in emotion perception. Moreover, attention and perception in developmental disorders, and especially Autism Spectrum Disorder, have always interested her: she graduated in Psychology curriculum Neuroscience with a final dissertation on the experimental project “A correlational study between autistic traits and drawing in children: evidence of a distributed fine-grained analysis”. She worked as research assistant at Basque Center on Cognition, Brain and Language (BCBL) in San Sebastian – Donostia (Spain) working on neuropsycholinguistic processes and ERPs and at Instituto Universitario de Neurociencia (IUNE-Neurocog) at University of La Laguna in Tenerife (Canary Island) participating in a project on neurostimulation in ASD subjects.

Riann Singh is a Lecturer in HRM at The University of the West Indies, St. Augustine, Trinidad. She has done independent and joint research on HRM in SMEs, the predictors and the darker side of embeddedness/workplace deviance, employee engagement and tourism perceptions. She has published works in The International Journal of Human Resource Management, The International Journal of Human Resource Development and Management, The Journal of Business Leadership, The Global Encyclopaedia of Public Administration and Public Policy, The Journal of Eastern Caribbean Studies, Caribbean Teaching Scholar, among other journals.

Martin Steinebach, born 1971 in Hanau, studied computer science at the TU Darmstadt from 1992 to 1999. In 1999 he became a PhD student at the GMD IPSI, in 2003 he received his PhD in Computer Science at the TU Darmstadt with a thesis on digital audio watermarks. In 2007, following the dissolution of IPSI, he moved to SIT, where he became head of the Media Security and Forensics department in 2010. Since November 2016, he has been an honorary professor at the TU Darmstadt, where his lectures include multimedia security. He is the author of over 170 publications. With his work on the ForBild

About the Contributors

project, Mr. Steinebach and his colleagues achieved second place at the IT Security Award 2012 of the Horst-Görtz Foundation. He leads numerous projects on IT forensics and big data security for industry and the public sector.

Larry Stewart currently serves as Executive Director and Associate Professor of Criminal Justice within the Criminal Justice and Police Sciences Program at Atlanta Metropolitan State College, Atlanta, Georgia. Prior to his current positions, he served as Associate Professor of Criminal Justice within the Criminal Justice Program at Savannah State University, Savannah, Georgia. He also served as Associate Professor and Program Coordinator for the Master's Degree Program in Public Safety Leadership within the Department of Leadership Studies, College of Continuing and Professional Studies at Mercer University, Macon, Georgia. He served as Dean, College of Public Safety Administration, St. Petersburg College, St. Petersburg, Florida, and Department Chair, Urban Affairs, Social Sciences & Social Work, University of the District of Columbia, Washington, DC. He holds the Doctor of Philosophy in Public Administration from the University of Southern California, Los Angeles, California.

Olivia Swee Leng Tan was a Legal Counsel of Kuala Lumpur Regional Centre for Arbitration (KLRC) and in charge of the Domain Name Dispute Resolution for both .com from Asian Domain Name Dispute Resolution Centre and .my cases at KLRC, as well as Mediation/Arbitration case management. She obtained her Bachelor of Law Degree with honours in 1993 from University of London (UK) and completed her Certificate of Legal Practise (CLP) in 1996. She was the book prize winner for the Civil Procedure Paper and General Paper awarded by the Certificate of Legal Practise Board (Malaysia) in 1996. She practised as an advocate and solicitor in Malaysia in the area of Corporate Litigation, Intellectual Property (Trademark), and Banking and Conveyancing. She continued to pursue her Masters in Law at the National University of Malaysia (UKM) in 2002. She obtained her PhD in Law at the National University of Malaysia (UKM) in 2014. Presently, she lectures Business Law, Corporation Law, Law for Engineers, Cyber Law, Media Law, Legal Informatics for Managers and Industrial Relations Law and also serves as the Director for Collaboration and Innovation Centre at Multimedia University (MMU) Malaysia.

Daniel Chaves Temp is a Lecturer at the Federal Institute of Science, Education and Technology Farroupilha (IFFar, Alegrete, RS, Brazil). He holds BS degree in Informatics from the University of the Region of Campanha (URCAMP, Brazil, 2009) and Specialization (2018) in Computer Networks. Cisco Certified Network Associate (CCNA) Instructor. His primary research interests include network security and management.

Poongodi Thangamuthu completed Ph.D at Anna University, Chennai and currently working as an Assistant Professor in Galgotias University, Greater Noida, Uttar Pradesh. She has 12 years of teaching experience in the field of computer science. Her area of interest lies in the field of Internet of Things, Big data, Blockchain, Networking. She has published more than 10 international journals and contributed book chapters.

Ciza Thomas is currently working as Senior Joint Director, Directorate of Technical Education, Government of Kerala, Trivandrum, India. She completed her B.Tech and M.Tech from College of Engineering Trivandrum and PhD from IISc, Bangalore. She was trained in Cyber Security at the Com-

puter Emergency Response Team (CERT) at US and also at Carnegie Melon University, Pittsburgh, US under Govt. of India scholarship. Her area of expertise is Network Security with research interest in the fields of Information Security, Data Mining, Sensor Fusion, Pattern Recognition, Information Retrieval, Digital Signal Processing, and Image Processing. She has publications in more than 40 International Journals and International Conference Proceedings. She has edited five books in the field of Sensor Fusion, Complex Systems, Data Mining and Ontology. She has published seven book chapters in the field of network security and pattern recognition. She is a reviewer of more than ten reputed International journals including IEEE transactions on Signal Processing, IEEE transactions on Neural Networks, International Journal of Network Security, International Journal of Network Management, and IEEE-John Wiley International Journal on Security and Communications Network. She is a guest editor of the IEEE Security and Privacy Magazine. She is a recipient of achievement award in 2010 and the e-learning IT award in 2014 from Government of Kerala.

Sachin Tiwari is doctoral candidate at the Centre for Canada, US and Latin American Studies (CCUS&LAS) at School of International Studies, Jawaharlal Nehru University (JNU), India. His research interest includes working on the issues of international relations, global governance particularly cybersecurity and its implications on security. He completed his M.A. in Political Science from Jamia Millia Islamia University, New Delhi, India. Later he completed his M.Phil. on dissertation titled 'US Search for Cybersecurity: Domestic and International Dimensions' in 2018 from JNU. He has published conference papers, articles and book chapters on topics prominently Contestation in Cyberspace and International relations, Cyber Policy, and aspects of US Foreign policy.

Curtis L. Todd is a professor of Social Work at Atlanta Metropolitan State College in Atlanta, Georgia, USA. His research and practice interests include child and family welfare, adult learners and distance education, first generation college students, retention and college completion programming. Other areas of scholarly inquiry include restorative justice, incarceration disparities and social control mechanism within criminal justice systems. He received his Western education, training and advanced degrees from Clark Atlanta University (Ph.D., Social Work Policy, Planning, Administration, and Social Science), the University of Georgia (M.S.W., Social Work) and Albany State University (M.S., Criminal Justice).

Deepak Singh Tomar obtained his B. E., M. Tech. and Ph. D. degrees in Computer Science and Engineering. He is currently Assistant Professor of CSE department at NIT- Bhopal, India. He is co-investigator of Information Security Education Awareness (ISEA) project under Govt. of India. Currently, he is chairman of cyber security center, MANIT, Bhopal. He has more than 21 years of teaching experience. He has guided 30 M Tech and 3 PhD Thesis. Besides this he guided 70 B Tech and 15 MCA projects. He has published more than 54 papers in national & international journals and conferences. He is holding positions in many world-renowned professional bodies. His present research interests include web mining and cyber security.

Zafeiris Tsiftzis (Ph.D, LL.M., BSc) is currently working as a legal advisor in UK civil litigation. He has already completed his doctoral studies in International Human Rights Law in the School of Law at the University of Bolton (Bolton, United Kingdom). His research interests are based on human rights law and humanitarian law and also on international law and international criminal. His doctoral research is on the international preventive framework for human rights abuses committed by private military and security companies.

About the Contributors

Pasi Tyrväinen is a Professor of Information Systems and the Dean of the Faculty of Information Technology at University of Jyväskylä. His background includes fourteen years at Honeywell and Nokia Research Center. He has 100+ publications on software business, enterprise content management, artificial intelligence, technology adoption etc. in EJIS, IST, JIE, JIM, JSS, DSS, IEEE Software and others.

Rizwan Ur Rahman obtained B.E and M.Tech in Computer Science from Maulana Azad National Institute of Technology (MANIT), Bhopal with Hons grade. His programming experience includes C/C++, C#, SQL, ASP, ASP.NET, VB, VB.NET; Win Forms, Web Forms and Java. He has worked on government projects and R&D department of CRISP. Currently he is an assistant professor in JayPee University, Solan, H.P., India . His area of research includes web programming and web security.

Rossanne Gale Vergara is currently a PhD candidate at Multimedia University, Malaysia. Her research area is in biometric data security regulation and policy. She obtained her Master of Business Administration “Multimedia Finance” from Multimedia University in 2018 and her Bachelor of Science in Oceanography from the United States Naval Academy in 2004.

Rishu Verma is B.Tech Student at JayPee University, Solan, India.

Michael Villano provides research computer consulting to the Department of Psychology at the University of Notre Dame. He is also the Assistant Director of the eMotion and eCognition Laboratory where he conducts research in human robotic interaction and applications of video game and robot technology to a variety of health and social issues. Current projects include investigating moral decision-making of drone pilots in a simulated 3D game environment with the United States Air Force Academy and the development and validation of a 2D game-based cognitive assessment tool for the United States Air Force School of Medicine. Dr. Villano is also the Co-Director of the Virtual Reality Laboratory where he has developed a VR simulation of an on campus building atrium for acrophobia therapy and a shopping mall for the study of prospective memory. Prior to returning to the academic environment, Dr. Villano conducted research and development for various industries in e-commerce, web-based electronic performance support systems, human-computer interaction, ergonomics and computer-based simulation and training.

Danish Wadhwa is B.Tech Student at JayPee University, Solan, India.

Lacey Wallace is an Assistant Professor of Criminal Justice at Penn State Altoona. Her research focuses on juvenile delinquency and substance use. Her work also includes an examination of family and peer processes that contribute to these behaviors.

Ping Wang is a Professor of Computer and Information Systems at Robert Morris University and a Certified Information Systems Security Professional (CISSP). He is also a Sun (Oracle) Certified Java Programmer and has over 10 years of consulting experience in Information Technology, E-Commerce, Cybersecurity, and served as a senior developer on a US Department of Defense grant project on Survivability and Information Assurance for three years. Dr. Wang has over 20 years of experience in teaching, research, curriculum development, and program management in higher education including most recently serving as Program Director and Professor of Cybersecurity in the University of Maryland system.

He has received three best paper awards for his publications on Cybersecurity at recent international conferences in addition to several other distinguished national and international awards for innovation, teaching, and research.

Veronica Wegner is a Neuroscience and Behavior Pre-Health Major, University of Notre Dame Class of 2019.

David Wesley is a lecturer and case research manager at Northeastern University's D'Amore-McKim School of Business, Department of International Business and Strategy. His research encompasses a range of strategic management topics, including international strategy, cultural diversity, intellectual property, and new product development. He has published more than 100 case studies and is co-author of *Innovation and Marketing in the Video Game Industry*.

Jessica Whitney earned her Masters of Science in Information Systems and Bachelors of Science in Marketing from San Diego State University where she was recognized as 2017's Most Outstanding MSIS graduate. She has received multiple awards for her thesis research which focused on the use of technology and knowledge management principles to help identify online human trafficking and the design of a decision support system for the effective response to technology-driven insight in this field. During her graduate studies, Ms. Whitney also worked as a Graduate Assistant in the Management Information Systems department at SDSU. She started her professional career with the County of San Diego in 2014 supporting the technology used by attorneys, support staff, and investigators in their pursuit to protect the innocent and prosecute the criminals. She has recently accepted a position working with law enforcement on data management and analytics.

Michelle F. Wright is a research associate at Pennsylvania State University. Her research interests include the contextual factors, such as familial and cultural, which influence children's and adolescents' aggression and victimization as well as their pursuit, maintenance, and achievement of peer status. She also has an interest in peer rejection and unpopularity and how such status relate to insecurity with one's peer standing, aggression, and victimization.

Szde Yu is an Associate Professor of Criminal Justice at Wichita State University. His specialization area includes cybercrime and computer forensics.

Nezer Zaidenberg completed his B.Sc (1999 CS and operations research), M.Sc (2001, Operations research) and MBA (2006, finance) from Tel Aviv University. Nezer completed his PhD in the university of Jyväskylä, Finland. (2012, faculty of IT) Nezer was awarded Docent from the university of Jyväskylä in 2013. Nezer was software engineering faculty member in Shenkar college, Israel and is currently a CS faculty member in the college of management academic studies, Israel. Nezer is also leading Truly-Protect a start-up developing hypervisor-based security solutions.

Index

A

Academic Cheating 180, 182, 192
 Active Measures 272-274
 Activism 4, 177, 212, 215-217, 248, 334, 336-337, 339, 346, 348
 Addictive Behaviour 616, 618, 627, 632
 Affiliate Marketing 1062-1064, 1073, 1075
 Alternative Facts 356
 Alternative Media Outlets 57, 64
 AMNSTE 1062-1063, 1067, 1075
 Anonymity 1, 5, 85, 112, 114-116, 119, 121-122, 124, 129-130, 132-133, 143-145, 147-148, 154, 156-158, 160-162, 170-172, 175, 180, 198, 244, 262, 310, 333, 374, 395, 398, 401, 403-405, 411, 462, 464, 468, 471, 518-519, 525, 547-548, 569, 572, 593-597, 608, 616-617, 640, 649-651, 659, 669, 691, 743, 770-771, 777, 780, 787, 856, 948-949, 990, 992, 1003, 1025, 1027
 Anonymization 156, 170, 229, 572, 575-576, 579, 777, 779-781
 Anonymous 5, 57, 64, 112, 114, 116, 118, 124, 129-130, 136-137, 146, 148, 154, 156, 164, 169-170, 180, 185, 249, 305, 309-310, 320-321, 323, 335-336, 338, 347-348, 350, 357, 402-403, 407, 454, 462, 465, 467, 471, 524, 572, 593, 606, 616, 629, 636, 640-641, 650-651, 668, 670, 691, 698, 758, 772, 787, 924, 992, 1004, 1006, 1090
 Anxiety 597-598, 618-619, 621-622, 634, 649, 659, 663, 669, 673-674, 692, 704
 API 794, 813, 822, 1071, 1154, 1157-1159
 ARM Architecture 1150-1151, 1161
 ARM Virtualization 1150, 1161
 Article Scraping 789, 791, 809
 Artificial Intelligence (AI) 28, 31, 34, 36-37, 124, 126, 196-197, 199, 231-232, 236-238, 240, 271, 278, 335, 352, 355, 360, 480, 570, 674-675, 678, 685, 758, 872, 877, 901, 914, 1034-1036, 1038, 1042, 1089, 1109

Attacks 1, 3-5, 7-17, 23-24, 26-30, 38-42, 44-46, 68, 93-96, 101, 104, 114, 116, 130-132, 137, 143, 157, 172, 194, 197, 199, 201-202, 204, 213, 235, 243, 245, 250, 258-259, 262-263, 267, 271, 274-279, 285, 288-290, 300, 332, 335-338, 342-343, 346, 370, 374, 376-377, 380, 383-385, 398, 404, 408, 412, 414, 448-450, 452-453, 455-456, 458, 461, 487, 607, 629-631, 637, 641, 701, 719, 738, 756, 762, 764-765, 767-768, 770, 777, 781-782, 788, 800, 807, 810-812, 816-820, 823, 825, 839-846, 859, 864, 867-871, 874, 877-878, 885-886, 894-898, 901, 905-907, 910, 914, 917, 922, 924-925, 928, 938, 964-965, 967, 969, 971, 978-979, 982, 990, 994, 1003-1004, 1008, 1021, 1027, 1029, 1061, 1072, 1077, 1083, 1085, 1088, 1109, 1113, 1118, 1138, 1140-1141, 1143-1146, 1151, 1158, 1161
 Audit and Policy Mechanisms 1052
 Auditing 236, 927-928, 931
 Automated Teller Machine 1022
 Avatar-Based Management 1034-1035, 1037-1039, 1042, 1044, 1052
 Avatar-Based Management Technique Use 1038, 1042
 Awareness of Cyber Hygiene 966, 969
 Axial Coding 64

B

Behavioral Biometric 1123, 1128
 Big Data 125, 196, 199, 237, 250, 258, 395, 481, 499, 517, 597, 718, 721, 730, 758, 859-860, 905, 915, 1048, 1089
 Bilinear Pairing 1114, 1119
 Bitcoin 9, 26, 40, 53, 55, 80, 114-116, 121, 125, 132-133, 142, 158-160, 164, 172, 403, 462, 466-468, 471, 476, 616, 773, 858, 885, 902, 921, 935, 945-960, 963, 1089-1091, 1096-1099, 1104, 1108, 1111

Blockchain 115-116, 123, 160, 396, 401, 467, 476, 772, 900, 902, 919-923, 927-929, 931, 947-948, 953, 963, 1044-1049, 1052, 1089-1091, 1101, 1104, 1107-1109, 1111
 Blue Pill 1136, 1138-1140, 1143-1148
 Blue whale 661-663
 Board Support Package (BSP) 1161
 Boot Loader 461, 1141, 1152, 1159, 1161
 Bootkit 1138, 1148
 Botmaster 1077-1079, 1083-1084, 1088
 Botnets 27, 29, 31, 132, 274, 285, 376, 380, 846, 898, 1077-1079, 1081-1086, 1088
 Bots 13, 26, 595, 789, 804-806, 816, 845, 866, 874, 877, 917, 1077-1078, 1080, 1084-1085, 1088
 Brightfield 639
 Bullying 7, 66, 213, 223, 323, 376, 540, 586, 592, 595, 598, 600, 609, 614, 619, 621, 627, 640-641, 643-645, 647, 649, 651, 659, 668-678, 685-695, 698, 703, 828, 1028, 1032
 BYOD 1123

C

CAPTCHA 794, 804, 865, 871-872, 877, 899, 917
 Cashless 932-934, 938-939, 942-943, 963, 1018, 1032
 Cashless Policy 1018, 1032
 Cashless transactions 932, 963
 Catfishing 608, 614, 825
 Cellular phone 694
 Certificate Transparency 905, 915, 917
 CFAA 340-341, 343, 407
 Chain of Trust 461, 1141-1142, 1148, 1151, 1158-1159, 1161
 Child Pornography 3, 7, 68, 125, 137, 158, 165, 172, 195, 200, 378, 402, 430, 463, 472, 519, 533-534, 536-537, 539, 541-542, 546, 564-565, 567-576, 579, 615-616, 618-619, 622, 627, 856-857, 859, 1030, 1032
 Child Prostitution 407, 533, 535, 538-539, 541-542, 546, 567
 Child Sex Tourism 519, 535, 541, 546
 Child Sex Trafficking 501, 535-537, 541-542, 546
 Clearnet 153, 155, 164, 171-172, 401, 472
 Click Spam 864-865, 880
 Clickbait 1053-1054, 1057, 1061
 Cloaking 865, 880
 Cloning 142, 703, 706, 832, 901, 1029, 1032
 Cloud Act 383, 385, 390
 Cloud Computing 23, 37, 718, 730, 763, 787, 902, 1124, 1150
 CNI 297-299, 303

Cold War 242, 247, 250-251, 255, 262, 265, 273, 275-276, 278, 350
 Collapsology 351, 360
 Collectivism 659
 Command and Control Server (CnC server) 1079-1083, 1088
 Commerical Cyberstalker 639
 Compromised Accounts and Stolen Data 882-883
 Computer Code 392-395, 397-398, 448, 931
 Computer Fraud and Abuse Act 340, 343, 346, 376, 407
 Computer-Assisted Cybercrime 194-195
 Computer-Focused Cybercrime 194-195, 200
 Confidence Romance Scams 76
 Consumer Trust 30, 32
 Contact-Driven Offender 557, 564
 Content Analysis 54, 630
 Content Scraping 788-790, 809
 Convention on Cybercrime 197, 374, 376-377, 381-382, 385-386, 419, 583
 Convention on the Rights of the Child 538, 541
 Conversational Analysis 352, 354, 360
 Conversion Faking 1069
 Conversion Hijacking 1069
 Conversion Stealing 1068-1069, 1071
 Convolutional Neural Networks (CNN) 1089, 1111
 Cookie Stuffing 1062-1063, 1066-1068, 1071
 Cookies 716, 730, 733-734, 742-743, 842, 898, 1029, 1062-1068, 1071, 1076, 1082
 Corporate Integrity 305
 Covert Communication 855-857, 860, 863
 CPA 1062, 1064, 1066, 1068, 1073, 1075
 CPC 1062, 1064-1065, 1068, 1070, 1076
 CPM 1062, 1064-1065, 1068, 1070, 1076
 Crawling 153, 164-165, 470, 486, 789, 801-802, 804
 Crime-Fake News 52-61, 64
 Criminal Justice Systems 334, 341-343, 606, 612, 701
 Criminal Negligence 332
 Criminalization 376-381, 568, 570
 Criminals 1, 15, 25-27, 29-31, 36, 45, 69, 108, 114, 131, 142, 144, 146, 158, 160-162, 193-194, 196, 199, 212-213, 223, 231, 237, 244, 315, 334, 341-342, 382, 397, 402-405, 413, 416-417, 419, 424, 426, 437, 446-448, 462, 471-472, 500, 518-519, 526, 607, 610, 632-633, 635, 699, 702-703, 706-709, 719, 767, 811-812, 824, 838-839, 852, 854-855, 857-859, 900-901, 905-906, 908, 910, 915, 979, 1003, 1019-1023, 1025-1027, 1031
 Criminological Theories 215, 223, 978
 Criminology 69, 211, 223, 375, 415, 606, 614, 825, 851, 860, 982
 Critical Discourse Analysis 347, 360

Index

- Critical Realism 73-74
Cross-Site Scripting (XSS) 8, 13, 842, 845, 847, 850, 868, 870
Crowdsourcing 480, 1056, 1061
Crypto 26, 133, 455, 458, 524, 772
Crypto Mining 26, 772
Cryptocurrency 8, 26, 114, 116, 142, 164, 466, 471, 476, 771-773, 858, 923-924, 927, 931, 935, 945-948, 958, 963, 1089, 1091, 1111
Cryptography 143, 158, 170, 392-393, 395, 398, 401, 454, 458, 467, 860, 945, 963, 1052, 1090-1091, 1105, 1112-1114, 1122
Cryptology 1089, 1108-1109, 1111
Cryptomarkets 462-463, 466-472, 476
CSEC 534
Cyber Abuse 606-612, 614, 686-687, 692
Cyber Attacks 1-3, 5, 7-8, 10, 15-18, 23-25, 29-32, 40, 131, 143-144, 196-198, 245, 251, 259, 261, 263, 267, 271, 274-281, 287, 298, 318, 327, 335-336, 374, 376, 382-383, 390, 396, 408, 435, 437, 444, 448, 690, 756, 764-765, 770, 773, 781, 787, 837, 839, 842, 847, 893, 964-965, 967, 970-971, 976, 978-979, 981, 983-985, 988, 1003, 1005, 1018-1020, 1024-1026, 1031-1032, 1109
Cyber Hygiene 965-971, 976
Cyber Law 6, 412, 415, 417, 437, 444, 532
Cyber Peacekeeping 287-289, 295, 298-300
Cyber Risk Perception 967
Cyber Security 1, 9, 16, 23, 25, 28-30, 267, 288, 290, 299-300, 414-415, 417, 419, 423, 434-437, 444-448, 525, 630, 636-637, 825, 867, 869, 906, 965, 968-969, 979, 983, 988, 1034-1035, 1037-1039, 1043-1044, 1052
Cyber Security Skills 988
Cyber Sovereignty 285
Cyber Threats 267, 380, 384, 417, 699, 707, 869, 887, 964-969, 971, 979, 982, 1010, 1077
Cyber VAWG 591-602
Cyber warfare 4, 242, 250, 259, 263, 267, 275, 287-290, 299-300
Cyber World 5-6, 19, 31, 608, 670, 702, 885
Cyberbully 669, 689-694, 698
Cyberbullying 24, 26, 537, 610, 614-616, 618-619, 621, 627-628, 630-632, 636, 640-651, 659, 668-678, 685-695, 698, 703-704, 706, 823, 979, 1028
Cybercrime Legislation 374, 376-377, 381-383, 418, 423, 425, 434
Cybercrimes 4, 7, 23-26, 29-32, 82, 85-86, 126, 223, 258-260, 265, 343, 375, 435-437, 444, 446, 448, 463, 472, 519, 525-526, 595, 622, 632, 636, 699-702, 704-705, 707-708, 825, 828, 906, 940, 980-984, 1019, 1029-1030
Cybercriminals 2-4, 10, 23-24, 26, 30-31, 40, 69, 77, 81-82, 85-87, 120, 131, 192, 194, 196, 203-204, 260, 342, 383, 392, 405, 607, 699-700, 705, 707, 709, 732, 738, 764-765, 837, 881-886, 888, 898, 901-902, 924, 990, 997, 1019, 1030-1031
Cyberharassment 703
Cyberhate 580-581, 586
Cyberlaws 526
Cybersafety 411
Cybersecurity 1, 10, 15, 23-24, 29, 38-40, 46, 66-67, 131, 142-145, 147-148, 197, 199, 203, 259, 262, 264-267, 287, 327, 333, 336-337, 340, 342, 348, 374, 377, 379-382, 384-386, 396, 402-408, 411, 415, 435, 446, 637, 708, 742, 781, 824-825, 886, 901-902, 964-969, 971, 979, 984, 990-995, 997-998, 1002
Cyberspace 6-7, 24, 26, 32, 35, 85, 108, 193-198, 202, 211, 244, 258, 262, 277-281, 286-288, 334, 336, 342, 348, 374-377, 379-380, 383-384, 392, 402-406, 408-409, 411, 414-415, 519, 532, 569, 571, 585, 607-610, 614, 619, 640, 650, 673, 689, 691, 702, 824-825, 851, 855, 965-966, 980, 982-984
Cyberstalking 24, 195, 198, 424, 430, 434, 610, 628-637, 639, 698, 701, 703-704, 706-707
Cyberterrorism 5, 343, 408, 414, 423-424, 428, 431-432, 434, 991
Cyber-Victimization 988
Cyber-Vulnerabilities 405, 411
Cyberwarfare 250, 285, 287, 378, 432
Cyberworld 5, 419, 423, 431
- ## D
- DAO 924, 927, 931
Dapps 927, 931
Dark Web 108, 110-112, 114-117, 119-126, 129-137, 140-145, 147-148, 152, 154-162, 164-165, 169-172, 175, 177, 185, 251, 259, 262, 327, 378, 390, 392, 394-396, 398, 401-409, 411, 462-463, 465-472, 476, 483, 518-519, 524, 529, 532, 572, 606-608, 614-617, 619, 622-623, 627, 633, 715, 765, 771-773, 816, 851, 854-856, 858-860, 863, 883
Darkfield 639
DARPA Memex 480, 485-486, 489
Data Breach 15, 27-28, 31, 39, 143, 201, 377, 380, 382, 414, 730, 732, 764, 837, 842, 884, 892, 966, 1003
Data Execution Prevention (DEP or W^X) 461
Data Protection 1, 31, 81-82, 85, 87, 126, 140, 249, 267, 300, 362, 366-369, 371, 380-381, 383, 395, 401, 432, 435-437, 442, 525, 731-732, 735-737, 739-743, 749, 752, 775-777, 779, 787, 902
Data Scraping 789-790, 796, 809

Data Theft 1, 132, 870-871, 1088
 Data Transfer 382-383, 790
 Database Scraping 788-790, 809
 DDR 303
 De George 307
 Death Groups 660-666
 Decipherment 1113, 1122
 Deep Learning 37-38, 42, 45, 278, 478, 481, 495, 758, 914, 1057, 1091
 Deep Net 771
 Deep Web 110, 112, 129, 136-137, 141, 143, 148, 153-155, 164, 177-178, 264, 392, 401, 404-405, 411, 462-464, 470-472, 476, 518-519, 524-526, 529, 532, 574, 576, 607, 616, 618, 627, 717-718, 771-772, 851, 992
 Denial of Service Attack (DDoS) 390
 Descriptive Statistics 144
 Deterrence 266, 271, 289-290, 375, 377, 381, 854
 Developed Country 420, 732, 747
 Developing Country 66, 732, 743, 747, 946, 949, 1020
 Developing Economy 945, 949, 951, 957
 Digital Age 240, 258, 443, 566, 1009
 Digital Cage 240
 Digital Currency 114, 132, 476, 772-773, 885, 931, 948, 1111
 Digital Evidence 197-198, 383, 551, 691, 698
 Digital Millennium Copyright Act (DMCA) 461
 Digital Psychology 673-674, 678, 685
 Digital Rights Management (DRM) 449, 461
 Digital Signature 435-436, 902, 1089-1091, 1095-1097, 1108-1109, 1111
 Digital wallet 932-933, 936, 938-941
 Discursive Ethos 355-357, 360
 Disidentification 235-236, 240
 Disinformation 107, 242-243, 245, 247, 249-251, 1055, 1058, 1061
 DMCA 450, 461
 DNS Pharming 843, 845, 847, 850
 Domain-specific Insight Graph 479-480
 Domain-Specific Search (DSS) 478, 483, 489-490, 495
 Drug Trafficking 133, 234, 265, 395, 462-463, 468-469, 472, 526, 825
 Drugs 113-114, 117-119, 121-123, 125, 130, 132-133, 142, 157, 159-160, 172, 244, 262, 326, 402-404, 462-464, 466, 469-472, 476, 519, 608, 616, 621-622, 663, 854-855, 859, 885, 948

E

E-Banking 828, 893-899, 902, 905-906, 908, 910, 915
 ECC 454, 810, 1091, 1112-1114

ECDSA 456, 1089-1091, 1097, 1108, 1111
 E-Commerce 1, 30, 119, 132, 159, 382, 397, 425, 437, 446, 466, 741, 750, 788, 790, 792-793, 803, 809, 825, 828, 839, 896, 898, 934, 938, 946, 1062-1068, 1070-1071, 1075-1076, 1125
 Economic Growth 95-96, 102, 107, 351
 Economic Impact 29, 365, 397
 Economic Prosperity 339, 407
 E-Culture 660
 E-Fencing 854-855, 863
 Electronic Health Records 774
 Elliptic Curve 454-456, 467, 1090-1097, 1099, 1101, 1112-1114, 1119, 1122
 Elliptic Curves Digital Signature Algorithm (ECDSA) 1089-1090, 1097, 1108, 1111
 Email Harvesting 789, 791, 809
 Email Spam 851-860, 863
 Embedded Systems 449, 1150
 Embodied Conversational Agent 675, 685
 Emojis 482, 498, 503-506, 509-510, 512, 514
 Empathy 357, 645, 650, 659, 671, 675-677, 690
 Encipherment 1113, 1122
 Encryption 9, 44, 110, 114, 130, 132, 144-145, 156, 169-170, 176, 264, 393-398, 401, 424, 452, 454-455, 462, 467-468, 472, 476, 572-573, 575-576, 579, 616, 633, 636, 752, 756, 772, 782, 840, 844, 846, 857, 860, 900, 902, 931, 1046, 1090, 1104-1105, 1107-1108, 1112, 1115, 1141, 1157
 Encryption-Decryption 1107, 1111
 Enron 317
 Entity Resolution 486-487, 495
 E-Payment 932
 Equal Rights 166, 176, 581
 Espionage 7, 199-200, 258-260, 262-268, 273, 275, 339, 342, 376-377, 381-383, 405, 407, 635, 762, 979-981, 1010
 ETag 1076
 Ethereum 922-924, 927, 931, 1091
 Ethics 140, 145-148, 178, 180, 184, 277, 279, 287, 300, 306, 309, 311, 313-314, 318-320, 323-325, 327-328, 333, 346, 355, 738-740, 819, 979
 Ethos 348, 355-357, 360
 Euclidean distance 1125, 1129, 1132
 European law 397
 E-Wallet 932-934, 936-940, 943-944
 Exploitation 16, 24, 67, 198-199, 243, 257, 265, 278, 376, 382, 386, 407, 497-498, 518-520, 523-524, 526-528, 532-542, 546-547, 549, 559, 565-571, 573, 575, 579, 591, 595, 606, 608, 619, 627, 787, 880, 984
 Externalizing Difficulties 659

Extraterritoriality 382, 385

F

Facebook 4, 27-28, 52, 58, 60, 137, 201, 245-248, 250, 259, 264, 354, 362-364, 366, 368, 383, 392, 395-397, 439, 443, 524, 526, 533, 581, 587-588, 592, 595, 599, 608, 615, 618-619, 621, 629, 631, 633, 635, 637, 643, 674, 677, 690, 699-701, 703-705, 707, 709, 716-720, 732-733, 742, 812-817, 823, 826, 828-829, 834, 935, 978, 983, 991, 1006, 1009, 1021, 1026-1028, 1056, 1065

Fake News 26, 28, 42, 52-61, 64, 263, 276, 278-279, 356, 392, 588, 615-616, 618-620, 622, 627, 1003, 1054-1058, 1061

Fake Reviews 1054, 1056, 1061

Fantasy-Driven Offender 552, 557, 564

FBI 15-16, 114, 116, 130-132, 143-144, 158, 263, 266, 336, 398, 403, 465-466, 534, 542, 713, 834, 845, 859

Fear of Missing Out (FOMO) 615, 618, 620, 627

File-Sharing 165, 172, 175, 572, 576

Financial Records 110

Firewall 31, 168, 412, 886, 908, 938, 980-981, 983, 1058, 1080, 1088

First Amendment 249, 264, 335-336, 366, 392-395, 397-398, 524, 570, 585

Forensics 82, 124, 143, 1019, 1136

Form Spam 864, 866, 876-877, 880

Forum 23, 87, 134-135, 159, 161, 202, 352-354, 366, 379, 412-413, 419, 470, 619, 642, 872, 874, 964, 991, 1008, 1021, 1025-1027, 1090

Fraud 3-4, 7, 24, 30, 66-69, 75-77, 79-82, 108, 119, 132, 135, 143, 181-183, 185-186, 188, 192, 195, 213, 216-223, 263-264, 304-305, 308, 310, 312, 315, 317-321, 324-328, 332, 339-340, 343, 346, 375-376, 378, 381, 407, 414, 428, 435-437, 443, 448, 478, 497-498, 517, 523-524, 527, 532, 608, 702, 720, 736, 738, 764, 824-825, 839, 852-854, 883, 886, 894, 898, 901, 905-906, 910, 912-915, 957, 980-983, 994, 1019-1020, 1023, 1062, 1066-1073

Fraudsters 125, 221-222, 810, 824-825, 828-830, 832, 894-895, 939, 1020-1030, 1063, 1069, 1071-1072

Free Speech 148, 263-264, 392-395, 397, 403-404, 407, 570, 671, 991

Freenet 156, 169-172

Frequency of Cyber Hygiene 966

Future Perspectives 894, 901

G

Gateways to Cyber Abuse 608, 614

GDPR 31, 126, 140, 143, 369, 380, 386, 395, 397, 401, 775-777, 787

Generalized Method of Moments (GMM Estimation) 107

Ghostwriters 179-182, 185-186, 192

Gini Coefficient 101, 107

Globalization 24, 30, 236, 242, 244, 251, 256, 520, 616, 1018

GlobalPlatform 1153-1154, 1158, 1161

Gnutella 167-169, 172

Governing 19, 31, 318, 362, 367, 385, 403, 591, 606, 735, 775-776, 787

Grey Zone Conflicts 271-273, 275-281, 285

Grey Zone Threats 285

Grooming 535, 539-541, 546, 549, 551, 553-555, 559, 564, 570-571, 574, 576, 579, 586, 595, 619

H

Hacker Culture 346-347

Hacker Ethics 346

Hacking 1-2, 4-7, 10-12, 26-27, 40, 66, 126, 133-134, 148, 155, 157, 159, 194, 198, 202, 213, 243, 259, 264, 273, 275, 318-319, 335-337, 339-340, 342-343, 346, 348, 350, 360, 375, 398, 407, 412, 419, 449, 454, 456, 470, 593, 595, 644, 700, 703, 719, 722, 737, 739, 764-765, 768, 781, 811, 823, 834, 882-883, 906, 965, 982, 990, 992, 1010, 1019, 1054-1055, 1089, 1101, 1108

Hactivism 334-337, 339, 342-343, 346-348, 360

Harassment 3, 68, 198, 236, 238, 264, 305, 326, 375, 435-436, 586, 591-600, 610, 628-632, 639, 641, 669, 677, 687, 689, 698, 700-701, 703-707, 823

Hate Speech 6, 247, 375, 580-582, 584, 587-588, 592, 594-595, 597, 1010-1011, 1054, 1058, 1061

Health Research Fraud 328, 332

Healthcare Fraud 319, 326, 332

HFI 993, 996, 1001

Homebrew 449-454, 456-457, 461

HPKP 917

HRM 314-315, 317

HSTS 917

HTML5 1065, 1072, 1076

HTTP Cookie 1063, 1065-1066, 1072, 1076

Human Behaviours 964, 971

Human Freedom Index 993, 1001

Human Safety 308

Human Sex Trafficking 497-501, 503-506, 508-511, 513, 517

Human Trafficking 3, 234, 472, 478, 480, 482-484, 486-487, 489-490, 495, 497-498, 500, 503-507, 518-521, 523-529, 532, 538, 856, 860

Hybrid Warfare 242-245, 251, 256
 Hypercall 1161
 Hyper-Computation (or Super-Turing Computation) 1034, 1042
 Hyperobjects 272, 278-279, 281
 Hypertext Transfer Protocol 15, 789, 1088
 Hypertext Transfer Protocol (HTTP) 15, 789, 1088
 Hypervisor 454-455, 461, 1136-1141, 1143, 1145-1146, 1148, 1150, 1152-1153, 1156, 1158-1159, 1161
 Hypervisors 1137, 1143, 1152-1153

I

I2P 110, 133, 156, 159, 169-172, 772
 ICT 66-67, 69, 75, 87, 197, 199, 212-213, 223, 298, 377, 382, 411, 415, 417, 435, 519, 524-526, 575, 594, 676, 686, 689, 694-695, 698, 700, 707, 709, 823-825, 991, 997, 1002, 1018, 1020, 1031-1032, 1112
 Identification Warning Signs 1017
 Identity Theft 3, 66, 68, 75-77, 82, 133, 195, 264, 376, 381, 383, 472, 595, 622, 630, 640, 738, 764, 823-825, 829-831, 834, 837, 839, 844, 847, 850, 882-883, 980-981, 983, 1022-1023, 1026-1027, 1032, 1125, 1127
 Identity-Based Encryption 1112, 1115
 Illegal Practices 307
 Indicators Of Compromise (IOCs) 197
 Individualism 659
 Information and Communication Technology (ICT) 66, 698, 824, 1112
 Information Extraction (IE) 481-482, 484, 486, 490, 495, 500
 Information Operations 275, 279, 285
 Information Sciences Institute 478
 Information Security 1, 10, 16-18, 38, 40, 108, 267, 379-380, 382, 406, 411, 622, 773, 781, 810-812, 817, 844, 867, 874, 894-895, 902, 920, 1035, 1038, 1052, 1112
 International Laws 285, 445, 518
 Internet Blocking 574, 576, 579
 Internet Crime Complaint Center (IC3) 15, 144, 699, 713, 859
 Internet Fraud 135, 143, 327, 957
 Internet of Things (IoT) 9, 23, 27, 35, 43, 126, 327, 342, 499, 716-717, 722, 730, 749, 758, 846, 869
 Internet Privacy 714, 716, 721, 732, 735, 738, 741-743, 747
 Internet Regulations 148, 585, 614, 737, 739
 Internet Relay Chat 1079, 1088
 Internet Research Agency 245

Internet Utilisation 742, 747
 Intimate Partner 606-612, 614
 Intrusion Detection Systems 25, 1077, 1088
 Intuitive Interface 486
 Investigative Schema 487, 489, 495
 Invisible Internet Project 110, 772
 IP Address 112, 114, 166, 168, 170-171, 175, 572, 616, 627, 806-807, 843, 845, 850, 1024, 1071-1072, 1112
 IRC 1077, 1079, 1088
 Isolation 405, 549, 551, 553, 555-557, 559-560, 564, 615, 621-622, 659, 673, 678, 921, 1009
 ITU 66-67, 87, 375-376, 378-379, 384-386, 414, 436

J

Jurisdiction 197, 248-249, 341, 364, 374, 382, 404, 406, 415, 442, 536, 538, 542, 573, 575, 584-586, 602, 737, 774-775

K

Key Exchange 1112-1113, 1115, 1118-1119, 1122
 K-FN 1125, 1129
 K-NN 1125, 1129, 1132
 Knowledge Graph (KG) 480-482, 486-488, 490, 495
 Knowledge Management 482, 498-499, 506

L

L4 1153, 1157, 1161
 Latent Variables 995, 997
 Leakage 328, 777, 1006, 1017, 1123, 1125, 1158
 Leakage Warning Signs 1017
 Legal Remedies 379, 574, 609-612, 705, 708
 Legislation and Enforcement 424
 Legislature 402, 404-406, 411, 1020
 Link Spamming 864-865, 880
 Load-time Click 1068
 Local Area Network (LAN) 756, 762
 LoM 994-998, 1002
 Loneliness 615, 618, 621-622, 645, 649, 659, 663, 665, 672

M

Machine Learning 28, 31, 35, 39, 42, 123-125, 160, 197, 395, 480-481, 483, 486, 495, 499-501, 504, 511-512, 514, 550, 673-674, 685, 758, 799, 805-806, 860, 874-877, 905, 914-915, 1010-1011, 1034-1039, 1042-1044, 1048, 1052, 1056-1058, 1078-1079, 1084-1086, 1089, 1101, 1108-1109,

Index

1129
Machine Learning Application 1038, 1042, 1052
Malicious Code 8, 13, 424, 429, 436, 448, 843, 845, 850, 870, 896, 901, 921
Malspam 858-859, 863
Malware 2, 8-9, 11-12, 18, 25-29, 31-32, 38-39, 43, 68, 132, 137, 160, 194, 199-200, 250, 259, 288, 293-294, 383-384, 390, 398, 402, 407, 448, 732, 764, 816, 823, 837-840, 842-843, 846-847, 858-860, 863, 869, 871, 883, 901, 907-908, 918, 964, 982, 1032, 1077-1080, 1084, 1088, 1157
Managerial Framework 308
Manhattan distance 1125, 1127, 1129, 1132-1133
Maoists 94, 96, 104, 107
Masquerading 342, 698, 855, 1080
Maturity Models 1052
Medical Data 154, 763-764, 770, 777, 782
Metropolitan Area Network (MAN) 756, 762
Misandry 580-581, 586-587
Misinformation 28, 247, 249, 1010, 1054-1055, 1061
Mobile Games 881, 885, 892
Mobile wallet 932, 934-935, 940, 942, 944
Mod Chip 449-451, 453, 458, 461
Modus Operandi 87, 193-197, 199-200, 202-204, 267, 471, 519, 630, 635, 639, 969, 971
Money Laundering 24, 43, 132, 159, 186, 234, 305, 312, 327, 616, 622, 772, 882, 884-885, 892
Monte Carlo Simulations 99, 107
Multistakeholder 377, 385-386
Mutual Legal Assistance (MLAT) 378, 390, 575

N

Nairaland Forum 1021, 1026-1027
Nation State 256, 300, 336
National Security 28, 30, 32, 53, 56, 143, 236, 242-243, 245, 250-251, 258, 261, 263-264, 268, 287, 334, 341, 343, 376, 393, 395-396, 404, 407, 446, 582, 719, 1065
Nationalism 256, 395
Nationalist 242-243, 250, 256
Netrespass 1019, 1032
New Media 347, 823
News Scraping 789, 791, 809
Nintendo 449, 452-454, 456-458
NIST 31, 290, 298, 1091
Nonconsensual Pornography 610, 614
Non-Technical User 489
Normal (Insecure) World 1151, 1154, 1161

Normative Belief 659

O

Object-Oriented Ontology 271, 279, 286
Offenders 57, 60, 72, 84-87, 193, 196, 198, 202-203, 341, 343, 376, 438, 443, 537, 539-542, 547-561, 564, 568, 572-573, 575-576, 606, 611, 614, 630, 633, 635-636, 668, 699-700, 703, 707, 709, 980-984, 1018, 1030
Onion 110, 112, 114, 121, 125, 130-132, 156, 164, 169-170, 176, 394-395, 398, 401-402, 462-465, 476, 519, 572, 616, 772
Onion Routing Project 110, 464
Online Ads 497-498
Online Child Sexual Exploitation 535, 540, 546
Online Communication 403, 581, 597, 650, 671, 690, 988, 1017
Online Criminal Activity 144, 881, 888
Online Expression 990-991, 1003
Online Games 593, 881-882, 884
Online Hate Crime 584, 586-587
Online Phishing 837-841, 843-847, 850
Online Privacy Protection 735, 845
Online Security 824, 834, 882, 908, 910, 970, 980, 994, 1008-1009
Ontological Approach to Cyberspace 286
Ontology 271, 279, 286, 487, 495, 498-499, 501, 503, 505-507, 509-512, 514, 517
Open Coding 64
Operating System 29, 31-32, 449, 454, 457, 461, 781, 796, 898, 966, 968, 1081-1082, 1137-1138, 1141, 1148, 1150-1154, 1156-1158, 1161
Optimism Bias 967, 976

P

Panel Data 100, 104, 107
Paper Mills 179-181, 183, 185-186, 192
Paradigm 23, 69, 73, 210-211, 222, 405, 461, 758, 1073, 1115
Parental Mediation and Monitoring 646, 659
Parenting Style 645, 659
Patient Safety 305, 318-321, 328, 332
Payment Gateway 963
Peer Attachment 645, 648, 659
Peer Contagion 648, 659
Peer Support 674-675, 685
Peer-to-Peer 123, 132, 156, 165-167, 172, 176, 466-

467, 534, 572, 935, 942, 945, 947-948, 953, 963, 1077, 1079, 1090-1091, 1108, 1111

Peer-to-Peer Networks 165-167, 534

Periodicity 1078, 1084-1086, 1088

Perpetrators 7, 60, 69, 74, 84-86, 198, 216, 223, 267, 277, 342, 466, 502, 519, 526, 565, 569, 572, 576, 580, 587, 593, 595, 597, 601, 608-609, 629-630, 633-636, 642-644, 668-669, 687, 689, 703, 706, 708, 771, 824, 830, 832, 834, 871, 887, 964-965, 969-971, 976, 1005-1006, 1009-1010

Personal Area Network (PAN) 756, 762

Perverved Justice 550-551, 564

Phishing 4, 8-9, 12, 15, 18, 26, 31, 38-42, 55, 132, 136, 143, 195, 201, 259, 275-276, 285, 376, 390, 448, 720-721, 730, 767, 814-815, 817, 823, 825, 831-832, 837-847, 850, 852, 866, 869, 871, 883, 896-897, 905, 907, 918, 939, 965, 980-981, 1003, 1019, 1032, 1082

Plagiarism 177-181, 184-188, 192, 324, 332, 825

Polarization 243-245, 247, 256

Police Force 58, 93, 99, 107, 418, 708

Policies 3, 5, 17-18, 60-61, 67, 81, 87, 101, 135-136, 142, 148, 177-178, 182, 184, 187-188, 214, 247, 273, 306-308, 310-314, 319, 321, 327-328, 333, 337, 364-365, 367, 371, 376-378, 380, 384-386, 407, 419, 470, 472, 497, 518, 521, 537, 581, 587, 595-596, 600, 622, 647, 688, 691, 693, 717, 737-738, 743, 773-774, 781, 812, 820, 824, 838, 844, 971, 991, 996, 1034, 1044

Political Reality 271-272, 275, 279

Political Warfare 271-272, 275, 285

Pornography 3, 7, 68, 125, 137, 158, 165, 172, 195, 200, 235-236, 378, 402, 404, 424, 430, 443, 463, 472, 519, 533-534, 536-537, 539, 541-542, 546, 564-565, 567-576, 579, 596, 601, 610, 614-616, 618-619, 622, 627, 704, 707, 737, 739, 828, 854-857, 859-860, 1018-1019, 1024-1025, 1030-1032

Poverty Head Count Ratio 101, 104, 107

Predictive Analytics 758, 1048, 1052

Price Scraping 788-790, 809

Prior Ethos 355-357, 360

Privacy Paradox 715, 721, 730

Privacy Protection 143-144, 172, 340, 405, 714, 720-721, 735, 747, 777, 845

Privacy Rights 140, 403, 409, 620, 736

Private Browsing Mode 720, 730

Private Cyberstalker 639

Private Health Data 763, 787

Privilege Ring 1148

Proof-of-Work 467, 772, 947, 963

Propaganda 4, 59, 107, 158, 165, 235, 242, 247, 249-

251, 259, 263, 272, 350-351, 355, 378, 392, 395, 582, 584, 620, 700, 1003

Prostitution 262, 266, 407, 507, 510, 519, 524, 528, 533, 535, 537-539, 541-542, 546, 567, 595, 1024, 1027

Protection Motivation Theory 69, 714, 730

Protection Orders 609

Provicim Attitudes 645, 659

Pseudo-Child 551-552, 564

Public Sphere 231, 234-235, 240

Q

Query Reformulation 485, 488, 495

R

Raising Concerns Policy 333

Random Forest 500, 511, 1084-1085, 1088

Random Forest Classifier 1088

Ransomware 390

Red Pill 1136, 1138-1140, 1144-1148

Regulations 1, 17, 19, 87, 148, 210, 248, 261, 272, 277-278, 281, 370-371, 397, 405-406, 565-566, 574, 581, 584-585, 587, 614, 629, 701, 718, 732, 737, 739, 773-774, 851, 854, 858, 970-971, 993, 1010, 1048, 1090

Relational Ethics 320, 333

Reporting 60, 123-125, 136, 182, 212, 217, 246, 263, 305, 308-312, 314-315, 318-321, 324-326, 328, 332-333, 376, 403, 417, 432, 522, 539, 587, 600-601, 610, 634, 643-644, 694, 705, 713, 773, 844, 895, 1048, 1124

Revenge Porn 137, 533-534, 537, 546, 567, 594-595, 610, 614, 704

Rich Execution Environment (REE) 1150, 1161

Risky Online Behavior 988

Romance Scams 75-76, 86, 608, 628, 636, 639

Rootkit 259, 285, 1136, 1138, 1140, 1148

Router 110, 114, 125, 156, 164, 170, 176, 394-395, 401-402, 462-464, 476, 519, 572, 772, 1080-1082, 1088

Routine Activity Theory 69-73, 83, 86-87, 979

RtoEx 994, 998, 1002

RtoExC 998, 1002

RtoExnonC 998, 1002

S

Scam 15, 55, 75-76, 86, 116, 119, 122, 135-136, 443, 716, 721, 814-815, 818, 837, 852-856, 858-860, 863, 1021-1024, 1026-1027, 1029

Index

- Scenography 347-349, 352-353, 355, 357, 360
Secure Communication 156, 1122, 1157
Secure World 1151, 1161
Security Breaches 15-18, 29, 31, 336, 722, 964, 1034, 1089
Select Committee on Deliberate Online Falsehoods 52-53, 60, 64
Selective Coding 54, 64
Session Hijacking 13, 843, 846-847, 850
Sex Crime 855
Sexting 533, 537, 542, 546, 570-571, 576, 579
Sextortion 534, 546, 570-571, 579, 587
Sexual Exploitation 24, 407, 497-498, 519-520, 523-524, 526, 528, 532-542, 546-547, 559, 565-569, 571, 573, 575, 579, 627
Shareable Content Object Reference Model (SCORM) 1042
SIEM 918
Signature-Based Classifier 1088
Silk Road 114, 116-117, 130-133, 136, 157, 159, 161, 403, 463, 465-466, 468-470, 616
Singular Value Decomposition (SVD) 1089-1090, 1101, 1111
Sleptsov Net (SN) 1035, 1042
Smart Contract 919-924, 926-929, 931, 1045-1047
Smart Contract Auditing 927-928
Smart Contract Vulnerabilities 919, 928
Smartphone 5, 533, 608, 635, 718, 816, 892, 901, 932, 939-940, 942, 956, 1125
Smuggling of Migrants 520, 523, 528, 532
Social Aberration 240
Social Comparisons 615-616, 618, 620-621, 627
Social Credit Score 609
Social Engineering 4, 9, 11-12, 18, 26-27, 38-39, 41-43, 135, 199, 201, 609, 765, 777, 791, 810-814, 816-820, 822, 831-832, 837-845, 847, 850, 871, 883-884, 896, 898, 900, 907, 918, 965, 969, 976, 979
Social Engineering Attack 9, 26, 765, 811, 817, 822, 837, 840, 847
Social Exchange Theory 993, 997, 1002
Social Exclusion 641, 659, 704
Social Media 53, 58, 60, 64, 76, 123, 137, 199, 232, 242-251, 259, 263-264, 275-276, 327, 337, 352, 362, 366-367, 374, 395, 411, 439, 471, 498, 503, 524, 533, 535, 540-541, 546, 560, 580-581, 585-588, 591-598, 600-602, 608, 614-615, 618, 620-621, 633, 635-637, 639, 643, 661, 669, 677, 686, 689-691, 694-695, 698-701, 703-704, 706, 708, 716, 720, 722, 750, 772, 810, 812-813, 815-816, 819, 823-831, 833-834, 840, 853, 884, 978, 982-984, 991-993, 1004-1010, 1021, 1025, 1027-1028, 1030, 1053, 1057, 1065, 1082
Social Media Identity Theft 824-825, 829-831, 834
Social Media Networking 608, 824, 834
Social Network 28, 120, 260, 267, 363-364, 369, 648, 662, 699, 717, 733, 742, 795, 810, 812, 814, 816-817, 819, 822, 824, 982, 984, 988, 1009
Social Network Security 822
Social Networking Sites 588, 600, 615, 618, 623, 627, 701-702, 709, 733, 810, 812-813, 816, 819-820, 825-830, 833-834, 978, 993
Social Networks 260, 262, 265-266, 354, 362-371, 499, 629, 661, 663, 665, 672, 674-675, 678, 713, 732, 735, 756, 758, 812, 817, 827, 829, 856, 873, 896, 979, 983, 1004, 1009, 1044, 1057-1058
Sociology of Crime 240
Sony Playstation 451
Spam 28, 132, 259, 274, 435-436, 448, 731-732, 736, 743, 851-860, 863-867, 872, 874-877, 880, 1023, 1056, 1058, 1077
Spamming 424, 429, 731, 736, 739, 791, 864-867, 872, 874-875, 877-878, 880, 1088
Spear Phishing 4, 12, 39-42, 275, 837, 839, 842, 850, 883, 1003
SSL 840, 908, 915, 917-918, 968
Stalking 3, 5, 7, 213, 223, 376, 586, 593, 595, 598, 608, 615-616, 618, 621, 627-636, 661, 687, 700, 830, 1019, 1032
Stateful Tracking 1076
Stateless Tracking 1072, 1076
Statutes 407-408, 424, 536, 610
Stealth 933
Steganography 573, 857-858, 860, 863
Stereotype 247, 257, 260, 582
Strategies 7-8, 16-17, 19, 66, 69, 73, 82, 85, 160, 167-168, 185-186, 197, 242, 267, 271, 276-277, 280, 285, 314, 338, 366-367, 377, 385-386, 417, 471, 549-550, 557, 559, 601-602, 606, 609-610, 612, 636, 646-648, 650-651, 659, 672-675, 688-689, 693-694, 781, 819, 838, 845, 929, 984, 1005, 1019, 1063-1065, 1069, 1077
Suicide 7, 26, 255, 595, 621, 649, 661-665, 704-705
Support Cyber Security 1037-1039
Surface Web 110, 112, 116, 118-119, 122, 129, 136, 152-156, 162, 164, 405, 411, 463, 476, 572, 574, 615-618, 622-623, 771
Surveillance 144, 156-157, 160, 233, 236, 240, 242, 258-259, 262, 341, 348, 350, 376, 383, 385, 392, 395-396, 398, 403, 407, 418, 431, 470, 598, 607, 630, 714, 716-717, 719, 772, 991
Sweetie 541
Switch 335, 353-354, 456-458, 464, 888, 1080-1082

1144, 1151, 1157

T

Target 2, 4-9, 12-15, 23, 25-26, 29, 38, 40-42, 44-46, 70, 72, 76, 83-87, 114, 121, 135, 145-146, 195-196, 199, 237, 242-243, 245, 248, 250-251, 256-257, 262-263, 266, 275, 278, 285, 336, 338, 408, 453, 467, 506, 519, 524, 540, 580-582, 606, 610, 617, 631, 640-641, 670, 672-673, 686-692, 694, 698, 703, 705, 720, 731, 737, 764, 768, 781, 811-812, 816-817, 819, 829, 832, 838-839, 842, 844-845, 850, 865-867, 872, 886, 895, 921, 952, 969, 979-983, 992, 1017-1019, 1021-1024, 1026-1027, 1030-1031, 1048, 1053, 1057-1058, 1063, 1073, 1137, 1139

Taxonomy 4, 278, 280, 495, 841, 865, 894-896, 1153, 1158

TChS 994-998, 1002

Technical Subterfuge 838, 840-842, 847, 850, 918

Technology Adoption 957

Teenagers 265, 567, 618, 622, 661-664, 674, 828, 1024

Terrorism 4-5, 7, 56, 93-95, 104, 108, 137, 263, 273, 340, 346, 350, 375, 379, 395, 397, 414, 425, 431, 472, 1017-1018, 1032

The Law of Armed Conflict 277, 285

The Onion Router (TOR) 164, 519

The TOR Browser 134, 156, 394, 401, 464, 466, 720

Theft and Sale of In-Game Items 882, 884

Thin Hypervisor 1137, 1148

Third-Party Applications 813, 822

Threat Assessment 196, 768, 1005, 1009-1011, 1017

Threats 1, 17, 29-31, 36, 39, 53, 126, 132, 140, 144, 148, 196, 199, 233, 235, 237, 242, 264-267, 285, 289, 293-294, 299-300, 327, 337, 343, 351, 374, 380, 384, 392, 398, 405-408, 417, 425, 444-445, 586, 591-592, 594-596, 598-599, 622, 629-630, 632, 634, 641, 660, 670, 688-689, 698-699, 701, 703-704, 707-708, 714-716, 730-731, 736, 744, 782, 788, 791, 812-813, 818, 820, 822, 843, 864, 867-869, 874, 881-882, 887-888, 893-896, 901, 908, 964-969, 971, 979, 982-983, 991-992, 1003-1004, 1006-1011, 1023-1024, 1034, 1043-1044, 1068, 1077-1078, 1150

Threshold 94, 215, 272, 277, 281, 510, 552, 780, 1091, 1127, 1131, 1138

TLS 756, 918, 1091

TMT 994-995, 998, 1002

Tor 110-112, 114, 116-117, 121, 124-126, 130, 132-134, 155-157, 159-160, 164, 169-172, 176, 394-396, 398, 401-402, 404, 462, 464-467, 471-472, 476, 519, 524, 572, 616, 636, 720, 772, 997

Tor Network 114, 117, 132, 156, 159, 170-172, 464-466, 471

Tourism 519, 535, 538, 541, 546, 567, 1068

Trade Secrets 108, 258, 261, 266, 338-339, 376, 395, 1140

Traditional Bullying 640, 668-672, 686-693, 695, 698

Traditional Face-to-Face Bullying 641, 644, 647, 649, 651, 659

Trafficking 3, 24, 133, 158, 185, 234, 265, 273, 340, 375, 395, 407, 462-463, 468-469, 472, 478, 480, 482-484, 486-487, 489-490, 495, 497-514, 517-529, 532, 535-538, 541-542, 546, 595, 707, 772, 825, 856, 860, 1019

Transhumanism 352, 360

Treatment 293, 299, 320, 324-326, 332, 339, 369, 537, 621, 630, 674, 676-678, 705, 758

Trusted Execution Environment (TEE) 1150, 1154, 1161

Trusted Platform Module (TPM) 1141, 1149

Trustzone 1150, 1150-1152, 1154, 1157, 1159, 1161

U

UN 248-249, 272, 288-290, 292, 295-300, 303, 376-380, 385-386, 419, 566, 568-569, 592-593, 599, 699, 868, 990, 1020

Unethical 125, 179-180, 182-183, 250, 304, 307-310, 313, 315, 317-319, 321, 325, 328, 332-333, 737, 739

Unethical Practices 313, 333

United Nations 194, 197, 244, 277, 288-290, 293, 295, 297, 303, 336, 340, 374, 377-378, 382, 384, 414, 416, 419, 463-464, 468, 470, 523, 527, 538-539, 541, 566, 582-583, 600, 699, 885, 990

US Constitution 249, 405

USA Patriot Act 340-341, 343, 346, 719

User Account 817, 822, 844

V

Veracity 58, 223, 333, 1053

Victims 2, 8, 26, 29, 31, 39-41, 43, 53-54, 69, 72, 74, 77, 84-86, 143-144, 198, 200-203, 222-223, 265, 321, 325, 338, 404, 407, 414, 417, 438, 471, 480, 497-505, 508-513, 518-524, 527-528, 536, 539-542, 547-551, 557, 559-561, 564, 566, 568, 572, 576, 580-581, 586-587, 594, 596, 598, 600-601, 606-607, 609-611, 621, 629-634, 636, 640, 642-645, 649, 659, 662-664, 668-675, 677-678, 691, 693-694, 700-701, 703-704, 706-709, 765, 767, 771, 813, 815, 823-825, 829-832, 834, 837-840, 842-845, 847, 850, 852-853, 855-856, 882, 885,

Index

905, 907, 924, 965, 969-970, 976, 980-983, 992,
996, 1011, 1022, 1024-1025, 1027, 1029-1030
Video Games 171, 449, 461, 594, 676, 881, 886, 892
Violent Extremism 1004, 1007-1011, 1017
Virtual Child Pornography 565, 567, 569-570, 579
Virtual Circuit 464, 476
Virtual Private Network (VPN) 10, 168, 401, 617,
627, 720, 730, 846
Virtual Reality 660, 665, 675-678, 685, 754
Virtue Ethics 184, 319-320, 333, 819
Virus 43, 108, 275-276, 663, 871, 908, 965, 1029
Vulnerability 17, 31, 38, 143, 198-202, 213, 223, 298,
351, 453, 518, 523, 527, 540, 688-689, 699, 716,
732, 768, 773, 781, 842, 865, 867-868, 880, 902,
924, 928, 965, 981, 1018, 1126

W

Warez 166, 168, 171, 176, 200
Warning Signs 1004-1005, 1010, 1017
Web Application Vulnerability 867
Web Bot 806
Web Robot 789
Web Scraping 506, 788-789, 792, 794-795, 798, 802,
804-805, 809
Web Security 842, 870
Web Spoofing 842, 845, 847, 850
Webcam 535, 541, 595, 1026
Well-Being 147, 246, 256, 305, 308, 615, 618, 622,
688, 692-693, 991
Whaling 842, 850, 979

Whatsapp 4, 395-396, 615, 631, 634-635, 637, 663,
716, 828-829, 1021, 1025-1027
Whistleblower 142, 147-148, 304, 306-307, 310-312,
315, 317-321, 323-328, 333, 338, 351
Whistleblowing 140, 148, 305-315, 317-324, 326-
328, 333
Wide Area Network (WAN) 756, 762
Wi-Fi 10, 699, 713, 762
Wii 453-456
Winmax 756, 762
Workplace Bullying 686-688, 690, 692, 694
Workplace Cyberbullying 686-695, 698
World Wide Web (WWW) 30, 137, 152-155, 161,
164-166, 318, 607, 616, 672, 685, 699, 713, 764,
771, 789, 806, 864, 1088

X

Xbox 451-452, 454, 457-458, 461, 885, 888, 892

Y

Youth 75, 87, 211, 214-221, 533-534, 537, 539-540,
542, 546, 575, 598, 646, 660, 664-665, 741, 960,
1019, 1027-1028

Z

Zigbee 756, 762